Best of TechEd 2013 Award Winners

Windows IT Pro

A PENTON PUBLICATION

JULY 2013 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

Licensing Simplified with System Center 2012

Windows Server 2012 Active Directory Claims Support

Integrate Hyper-V and vSphere Management

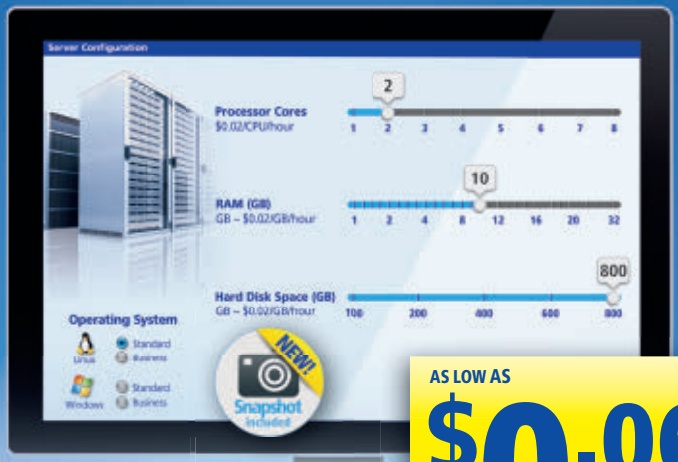
Michael Otey Top 10 Steps Microsoft Should Take to Fix Windows 8

Sean Deuby on Secure Cloud Computing



1&1 DYNAMIC CLOUD SERVER

PRICE CONTROL



AS LOW AS

$0.06

PER HOUR*
PLUS $60 OFF
FIRST MONTH

COMPLETE COST CONTROL

- **Full transparency** with accurate hourly billing
- **Parallels® Plesk Panel 11 included,** with unlimited domains

FULL ROOT ACCESS

- The complete functionality of a root server with dedicated resources

MAXIMUM FLEXIBILITY

- Configure the Processor Cores, RAM and Hard Disk Space
- Add up to 99 virtual machines

FAIL-SAFE SECURITY

- Redundant storage and mirrored processing units reliably protect your server

OPTERON PROCESSOR AMD

SUSE

Parallels Plesk Panel

1&1®

MEMBER OF united internet

DOMAINS | E-MAIL | WEB HOSTING | eCOMMERCE | SERVERS

Call **1 (877) 461-2631** or buy online

1and1.com

* Other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Customer is billed monthly for minimum configuration ($0.06/ hour * 720 hours = $43.20/ month minimum). A $60 credit (valid only for the first month) will be applied to your first month of service. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners. © 2013 1&1 Internet. All rights reserved.

AvePoint®

Collaborate with Confidence

Best of TechEd North America 2013 WINNER

Product Awards Produced By: Windows IT Pro

The Leader in **Compliance**, **Governance**, and **Management Solutions**

for Social Enterprise and Collaboration Platforms since 2001



Passion. Dedication. Excellence.

Resolve the confusion and chaos of today's disruptive technology trends with AvePoint.

www.avepoint.com

JULY 2013 / VOL. 19 / NO. 7

COVER STORY ▼

Understanding Microsoft System Center 2012 Licensing

— John Savill

With System Center 2012, Microsoft has completely changed how System Center is licensed for the management server, managed servers, desktops, and other hardware on the network. 21



Features

29 **Enable Claims Support in Windows Server 2012 Active Directory**
Sean Deuby

39 **Integrating Hyper-V and vSphere Management**
Michael Otey

Products

65 **Best of TechEd 2013 Award Winners**

69 **New & Improved**

Interact

51 **Reader to Reader**

60 **Ask the Experts**

In Every Issue

73 **Advertiser Directory**

73 **Directory of Services**

73 **Vendor Directory**

Chat with Us

Facebook Twitter LinkedIn

Columns



7 Need to Know

Microsoft and the Cloud OS v.Next
Paul Thurrott



13 Windows Power Tools

Bye-Bye Diskpart: PowerShell Is Moving In!
Mark Minasi



16 Top 10

10 Steps Microsoft Should Take to Fix Windows 8
Michael Otey



19 Enterprise Identity

Attention, IT Pros: You Can Help Evolve a Secure Cloud, Too
Sean Deuby

Editorial
Editorial Director: Megan Keller
Editor-in-Chief: Amy Eisenberg
Senior Technical Director: Michael Otey
Technical Director: Sean Deuby
Senior Technical Analyst: Paul Thurrott
IT Community Manager: Rod Trent
Systems Management, Networking, Hardware: Jason Bovberg
Scripting: Blair Greenwood
SharePoint, Active Directory, Security, Virtualization: Caroline Marwitz
SQL Server, Developer Content: Megan Keller
Managing Editor: Lavon Peters
Editorial SEO Specialist: Jayleen Heft

Senior Contributing Editors
David Chernicoff, Mark Minasi, Tony Redmond, Paul Robichaux, Mark Russinovich, John Savill

Contributing Editors
Alex K. Angelopoulos, Michael Dragone, Jeff Fellinge, Brett Hill, Dan Holme, Darren Mar-Elia, Eric B. Rux, William Sheldon, Curt Spanburgh, Bill Stewart, Orin Thomas, Douglas Toombs, Ethan Wilansky

Art & Production
Senior Graphic Designer: Matt Wiebe
Director of Production: Dylan Goodwin
Group Production Manager: Julie Jantzer-Ward
Project Manager: Adriane Wineinger
Graphic Specialist: Karly Prickett

Advertising Sales
Technology Market Leader: Peg Miller
Key Account Director: Chrissy Ferraro • 970-203-2883
Account Executives: Megan Key • 970-203-2844
Barbara Ritter • 858-367-8058
Cass Schulz • 858-357-7649

Client Services
Senior Client Services Manager: Michelle Andrews • 970-613-4964
Ad Production Coordinator: Kara Walby

Marketing & Circulation
Customer Service • 800-793-5697
Senior Director, Marketing Analytics: Tricia Syed

Technology Division & Penton Marketing Services
Senior Vice President: Sanjay Mutha

Corporate
Chief Executive Officer: David Kieselstein
Chief Financial Officer/Executive Vice President: Nicola Allais

Penton

List Rentals
MeritDirect
333 Westchester Avenue,
White Plains, NY 10604

Reprints
Reprint Sales:
Wright's Media • 877-652-5295

Windows IT Pro, July 2013, Issue No. 227, ISSN 1552-3136. *Windows IT Pro* is published monthly by Penton. Copyright ©2013 Penton. All rights reserved. No part of this publication may be reproduced or distributed in any way without the written consent of Penton.

Windows IT Pro, 748 Whalers Way, Fort Collins, CO 80525, 800-621-1544 or 970-663-4700. Customer Service: 800-793-5697.

We welcome your comments and suggestions about the content of *Windows IT Pro*. We reserve the right to edit all submissions. Letters should include your name and address. Please direct all letters to letters@windowsitpro.com. IT pros interested in writing for *Windows IT Pro* can submit articles to articles@windowsitpro.com.

Program Code: Unless otherwise noted, all programming code in this issue is ©2013, Penton, all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton, under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication.

Windows IT Pro



NEW CONTENT – GREAT NETWORKING – FUN!

IT/Dev CONNECTIONS

HTML5 · Visual Studio · ASP.NET · Windows Azure · Exchange · SQL Server · Cloud · Share Point

Mandalay Bay, Las Vegas
September 30 – October 4, 2013



Paul Thurrott



Mark Minasi

Join Microsoft & industry experts at this year's IT/Dev Connections and learn all new content from more than 175+ sessions! Topics include HTML5, ASP.NET, Exchange, SQL Server, Windows, Windows Server, Visual Studio, Windows Azure, SharePoint, Cloud, and Office 365.

Go to DevConnections.com to register.

Microsoft and the Cloud OS v.Next

At its annual TechEd confab in New Orleans in June, Microsoft announced a sweeping set of updates to its on-premises servers and cloud-hosted services that provided a first peek at the firm's plans to service these products. Known collectively as "Cloud OS"—more a vision than a product name—this group of products and services is Microsoft's answer to the trends sweeping our industry.

For simplicity's sake, I'll refer to this coming set of updates to the Cloud OS products and services as Cloud OS v.Next. But as you'll see, the on-premises servers are mostly going to be branded with R2 suffixes, as is the custom of Microsoft's Server & Tools business. And the Windows Azure services, as cloud services, don't really pick up any easily identifiable version number at all.

I first wrote about Cloud OS late last year, in "Microsoft's Cloud OS: A Vision of Infrastructure's Future." To make a long story short, Microsoft is evolving its on-premises servers to what it calls private cloud solutions, and Azure, Office 365, and other related services are public cloud solutions. Cloud OS is an acknowledgement that these products and services will evolve together in a virtuous cycle where each affects the other. Microsoft being Microsoft, the firm also offers hybrid solutions that bridge the two worlds, an important differentiator and advantage over its erstwhile competition.

Looking ahead to Cloud OS v.Next—again, this is my naming, not Microsoft's—we see a not-too-subtle move to a cloud orientation. While Microsoft continues to offer both on-premises and pure cloud solutions, and will do so for the foreseeable future, even its locally installed servers will be updated and serviced as if they were cloud services. This mimics how Microsoft is evolving core client-side products such as Windows and Office.



Paul Thurrott

is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows, a weekly editorial for *Windows IT Pro UPDATE*, and a daily Windows news and information newsletter called *WinInfo Daily UPDATE*.

Email

Twitter

Website

I've argued elsewhere—in "Azure Is the Future of Microsoft," specifically—that Microsoft's long-term goal is to fully embrace its "devices and services" mantra and move inexorably to cloud services in lieu of on-premises designs, and that Azure is thus, going forward, the primary business of the company. The Cloud OS v.Next updates, which will be delivered by the end of 2013 and will constitute the first wave of an ongoing series of updates to the current-generation products, don't represent that type of change, not yet. But they are the building blocks for the changes to come.

This means a consistent platform that spans on-premises infrastructure, Microsoft-hosted cloud services (Azure, Office 365, Windows Intune, and more), as well as service provider–hosted cloud infrastructure. This platform provides flexible development, unified management, common identity, integrated virtualization, and a complete data platform, Microsoft says, while providing choices to customers.

Looking at the specific products that make up Cloud OS v.Next, we see updates to core on-premises products such as Windows Server 2012 R2, System Center 2012 R2 (including Configuration Manager 2012 R2), SQL Server 2014, and Visual Studio v.Next, among others. In the cloud, you'll see updates and improvements such as Windows Azure Services for Windows Server 2012 R2 (my vote for silliest Microsoft product name this decade; guys, how about just calling it Azure Connect?), Windows Intune v.Next, and updates to Azure SQL Database, Azure Active Directory (with identity and access management), Azure Active Authentication, and more.

Beyond that, Microsoft promises "regular" cloud and on-premises releases—which I take to mean "yearly"—with common R&D across both environments. I've heard that Cloud v.Next + 1 could be a major release and could include the rebranding of all Azure services to remove the Windows moniker.

Before getting into specifics about Cloud OS v.Next, I would like to address the standard resistance that pops up around cloud computing, especially when you consider that these products point to a

future in which on-premises computing is potentially deemphasized over time. (That's not happening with Cloud OS v.Next.)

Microsoft distinguished engineer Jeffrey Snover explained that Microsoft would persuade customers to make the journey to the cloud by offering great performance with cloud costs, the promise of its Trustworthy Computing initiative, and what he calls Cloud Plug and Play. Under this system, you should be able to plug devices into the cloud anytime and anywhere, and access apps, data, and people. Plug applications—on Windows or Linux—into the cloud. Plug any resource into the cloud fabric: servers, storage, networking, whatever. And it should all just work. "This is our vision," he said. "This is where we're going."

Here's a peek at what you can expect from the Cloud OS v.Next updates. My *Windows IT Pro* compatriots, Sean Deuby and Mike Otey, have written articles that go into more detail about these changes.

Hyper-V: The Technology that Drives It All

Hyper-V in Server 2012 focuses on private cloud, and it's been well-received thanks to key functional updates such as Hyper-V Replica, Shared Nothing Live Migration, SMB 3.0 support for virtual machines (VMs), full Windows PowerShell support, and more. Today's Windows Azure actually uses the same Hyper-V virtualization services built into Server 2012, providing full VM interoperability between on-premises Hyper-V in Server 2012 and the Infrastructure as a Service (IaaS) capabilities of Azure.

Things are getting interesting with Cloud OS v.Next and the coming version of Hyper-V—Microsoft refuses to call it Hyper-V 4 or Hyper-V 3 R2 or whatever—and some intriguing capabilities emerge. First up is support for a new type of VM called Generation 2 VM. These VMs don't support any legacy hardware features and instead are UEFI-based, with much deeper integration with the underlying OS. A Gen-2 VM supports only 64-bit versions of Windows 8 and Server 2012 and later, and provides advantages such as Secure Boot

support, enhanced VM interaction with full Remote Desktop capabilities, and—admins will love this one—automatic product activation when run on Windows Server 2012 R2 Datacenter.

Hyper-V v.Next also supports live migration of VMs from Server 2012 to Server 2012 R2, faster Live Migration of VMs (2x improvement in time, Microsoft says, with SMB Direct support for those with high-end networks), and online VHDX resizing capabilities. You can also export a VM or VM snapshot while the VM is running.

Windows Server 2012 R2

I didn't get a full rundown of new Server 2012 R2 features, but in addition to the Hyper-V improvements already mentioned, there some major changes coming to the system's storage capabilities. Here, too, the original Server 2012 release offers a good story, with such technologies as Storage Spaces, SMB 3, data deduplication, Virtual Fibre Channel, ReFS, VHDX, and more. Server 2012 R2 is picking up some new and improved storage features, though the feature list is trimmed to accommodate the new yearly release cycle. It's also "cloud optimized," with support for private, public, and hosted clouds, and a new standardized management interface for storage management.

I'm particularly interested in the improvements to the well-received Storage Spaces feature, which lets you deploy redundant, off-the-shelf storage in ways that are more flexible and less complex than previous methods. With Server 2012 R2, Storage Spaces picks up a new Storage Tiers feature that piles on the performance: Here, you can specify a tier of SSD-based storage and a separate tier of traditional HDD storage, and create what is effectively a hybrid pool with optimized data placement. You can "pin" files—under admin control—to be on the SSD tier for speed, for example, and move data between tiers as required (or under a schedule). Storage Spaces is also getting a new write-back cache feature that helps absorb spikes in random disk write activity by essentially using an SSD tier as a buffer for the slower HDDs. It's particularly well suited for virtualized environments, according to Microsoft.

On the networking front, Server 2012 added many important features as well, including NIC teaming, SMB 3 multi-channel and SMB Direct, Quality of Service (QoS) features, IP Address Management (IPAM), and much more. For Server 2012 R2, Microsoft is improving NIC teaming with dynamic teaming capabilities that distribute loads more intelligently than before, improving IPAM for virtualized data centers, and adding a new feature called Virtual RSS (vRSS) that makes it easier to virtualize network-intensive physical server workloads.

Linux and UNIX Support

When it comes to Microsoft, Linux and UNIX aren't exactly the first thing that comes to mind, but the firm understands that the world is heterogeneous and that many organizations have Linux and UNIX too. Microsoft's goal here is simple: Play well with others and be particularly open in the cloud by embracing open standards and open source, and by enabling open source on its platforms.

I know, crazy talk. But Microsoft feels it can offer a superior private cloud infrastructure that supports both Windows (Server) and Linux (server) guests with a single systems management infrastructure that supports Windows (Server), Linux (server), and UNIX (server) as well. So while it's not completely altruistic, the result is pretty impressive: production-ready Linux and UNIX capabilities across Windows Server, Azure, and System Center.

Microsoft supports several Linux and UNIX OS variations—Red Hat, SuSE, CentOS, Ubuntu, Debian, and Oracle in the Linux space, and AIX, HP-UX, and Solaris UNIX—and, just in case you've not been paying attention, it's been doing so for four years. New to Server 2012 R2 are features for Linux guest VMs such as dynamic memory, dynamic virtual hard disk (VHD) and VHDX resizing, and remote VM replication for disaster recovery. (Interestingly, Microsoft's Linux Integration Services are actually delivered as part of the supported Linux distributions, not directly from the Microsoft website.)

Microsoft is also adding some System Center 2012 R2 features for managing Linux VMs, including online backup with Data Protection Manager and prebuilt Linux OS templates for private and public cloud deployments.

System Center 2012 R2

Speaking of System Center, the next version of Microsoft's systems management solution will fully support hybrid environments that work across Server 2012 R2 on-premises and Azure in the cloud. This includes hybrid networking features, which add up to what is essentially virtual networks that span the environments, hybrid identity including an update to Azure Active Directory, and hybrid data recovery functionality through the Windows Azure Hyper-V Recovery Manager, which provides Software as a Service (SaaS)–based recovery orchestration and management.

Windows Server 2012 R2 Essentials: Small Businesses

I was interested in Microsoft's plans to extend Windows Server 2012 R2 Essentials—the next version of its new line of small business offerings—up market, to include midsized businesses. Server 2012 R2 Essentials supports more PCs and devices, integrates with more services—including Office 365 as before, and also with Azure Active Directory and Azure-based Microsoft Online Backup—and is optimized for hosters with its new VM-based installation option.

I'll be writing more about Server 2012 R2 Essentials after I've had a chance to install it. Based on demos I've seen, it looks solid.

What's Next

The Cloud OS v.Next lineup is an intriguing bridge between the on-premises world and the cloud computing future. It's impressive for one year's work. At the time of this writing, I've spent a few days investigating this wave, but I'll say much more in the months ahead. ■

Bye-Bye Diskpart: PowerShell Is Moving In!

Don't miss these time-saving shortcuts

I've been doing a lot of Active Directory (AD) PowerShell coverage, and I aim to continue, but this month I want to take a break and talk about some truly cool PowerShell cmdlets: the *volume* cmdlets, the *partition* cmdlets, and the *disk* cmdlets. Why do I love them? They save me time—lots of time. But there's one wrinkle: They're available only on Windows 8 and Windows Server 2012. But if you're working with either OS, you shouldn't miss these. So here's a short rundown of three of those valuable commands.



Mark Minasi

is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

Email

Twitter

Website

Get-Volume: No Need for Explorer

At least once a day, I need to know what drive letters are free and which I'm using on my system. For ages, I've either opened up Windows Explorer or opened Diskpart and typed *list volume* (or its short version, *lis vol*). But Explorer requires the mouse, and Diskpart takes time to start up, and that slows me down. If, by contrast, I go to the PowerShell command prompt window—where I get much of my work done anyway—I need only type

```
get-volume
```

and I'll get a quick list of all currently used drive letters. (There's also a bunch of other information, but that's another story.)

Set-Partition: Relettering Drives without Diskpart

Get-volume has a cousin cmdlet, *set-partition*, that's also pretty useful. I'm usually curious about the currently used drive letters because

I want to change some partition's drive letter. For example, on my system, VMware Workstation gets cranky if the virtual machines (VMs) that I run aren't in a folder named *VMs* on a drive letter of E, and that volume is usually on a second physical drive. But because I have different combinations of storage devices attached on different days, the drive containing the VMs doesn't always get to be E. (Yes, there is a way to resolve that with *mklink*, but that too is a story for another time.) As a result, some days my first order of business is to get the E issue straightened out.

It's not unusual for me to find my *VMs* folder on, say, drive G, and something else—a USB stick, perhaps—on drive E. The fix isn't hard (re-letter the USB stick to something like V, freeing up E and enabling me to change the thing currently lettered as G to E). The problem lies in changing a partition's letter. You know what I mean: I have to fire up either Disk Manager or, worse, Diskpart.

Don't get me wrong, I love Diskpart. I couldn't have built my free replacement for Microsoft's SteadyState—which I call SteadierState—as a few batch files without it, but honestly getting anything disk-wise done with Diskpart always feels like I'm trying to build a mnemonic circuit with just stone knives and bearskins. Its syntax is highly idiosyncratic and reminds me of that weird Cisco IOS look to Netsh, another powerful command-line tool that no one uses because it's so hard to figure out, and scripting it is a pain.

In contrast, PowerShell cmdlets are a bit long-winded, but they're easy to read, as in these two, which solve my VMware problem:

```
set-partition –driveletter E –newdriveletter V
set-partition –driveletter G –newdriveletter E
```

Very nice, and trust me: If you've got the PowerShell command prompt already open and remember to use tab-complete, you can bang out those three commands (remember that you need a *get-volume* beforehand) much faster than opening Disk Manager, even with the

Windows key + X combination that you can use in Windows 8 and Windows Server 2012.

Get-Disk: More Diskpart Replacement

Many storage-related tasks require knowing not a drive letter but a drive number. Now, of course, in that sentence I (deliberately) made a mistake that we all tend to make: using the word *drive* or *disk* to sometimes mean a physical disk and sometimes mean a volume/partition. Most of us would say that we "installed a new drive" and in the next breath might refer to "data on drive G," where the first phrase refers to an actual physical drive and the second refers to a volume or partition. (Heck, even PowerShell does this. Look at the *-driveletter* and *-newdriveletter* parameters.) But here's one more PowerShell cmdlet that's worth learning when you're working with storage, especially if you want to avoid Disk Manager or Diskpart:

```
get-disk
```

This cmdlet shows you physical devices (mostly) and their disk numbers—one fewer trip to Diskpart. Give these cmdlets a try, and I think you'll see what I love about them! ■

10 Steps Microsoft Should Take to Fix Windows 8

Windows 8 suggestions from customers



Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro*.

Email

I haven't been a Windows 8 basher, but I'm also no Windows 8 fan. Microsoft's latest client OS has received a cool reception—and right or wrong, Windows 8 shoulders much of the blame for the sharp 13.9 percent decline in PC sales reported by IDC.

News about Windows 8 and the pending Windows Blue update have made it clear that Microsoft isn't going to address some of the key features that customers dislike about Windows 8—which is ironic considering that Microsoft claims to have a customer-centric focus. Here are the top 10 changes Microsoft should make to Windows 8 to increase the OS's number of fans.

1 Bring back the Start menu

Removing the Start menu was the biggest mistake Microsoft made in Windows 8. Leaving the Start menu in wouldn't have hurt anything and it would have made the new OS easier for existing Windows users to adopt. Instead, Microsoft chose to make Windows 8 users' lives difficult. Returning the Start menu would fix the biggest mistake in Windows 8 right away. The upcoming Blue release has been rumored to include the Start button, but not the Start menu.

2 Add touch support using Kinect

Windows 8 was designed around a touch interface and it's definitely more usable on a touch-enabled device. The only problem is, few people have touch-enabled devices. Plus, there's the disgust most people have with other people leaving greasy smudge marks on their device screen. Making a Kinect add-on for Windows 8 would

solve both problems by eliminating the need to purchase completely new touch-enabled monitors and by providing a gesture-enabled add-on that allows touch to work without users actually having to touch the screen.

3 Dynamically detect the device and boot accordingly

One of the other annoyances in Windows 8 is the inability to boot into the desktop. The desktop is where most users with standard PCs and laptops are going to spend most of their time. If Windows 8 is running on a tablet, then it makes sense to boot into the new Start screen. If Windows 8 is running on a non-touch device, then provide the option to allow the boot into the desktop. The upcoming Blue release is rumored to allow booting into the desktop, but it would be even better if the system could detect the type of device and boot accordingly.

Removing the Start menu was the biggest mistake Microsoft made in Windows 8.

4 Make everything visible

One of the strong points about Windows 7 and earlier interfaces is that you can eventually find everything by clicking on the different options you can see on the screen. That's not true in Windows 8. Menus appear and disappear depending on where you mouse or touch. Many people—especially ordinary folks—find this very confusing, and it could easily be rectified by adding Start screen or desktop icons for these sometimes invisible options.

5 Eliminate the reliance on keyboard shortcuts

Unlike any earlier edition of Windows, Windows 8 is not really usable without mastering keyboard shortcuts—at least not on a regular mouse- and keyboard-equipped PC. I can't count the number of times I now use Ctrl + X and the Windows key in a day. Keyboard shortcuts are great, but the point-and-click method is what made Windows popular in the first place. Again, surfacing regular tasks to the interface would make it easier for ordinary users.

6 Make the Start screen cooler

I know the Start screen has its fans, but it reminds me of the days when Visual Basic (VB) first came out and everything had to be too simple, too colorful, and too gauche. I liked the Windows 7 transparency and snap features. Windows 8's blocky nature seems like a step backward for a PC. Transparent, resizable, and floating tiles would be cooler.

7 Allow Windows 8 apps to run in a window

It seems silly to me that an OS called Windows can't run new apps in a window. Without third-party software, apps have to run in full-screen mode. Full-screen apps make sense for a phone, or maybe a small tablet, but nothing is less attractive than a single app stretched across my 27" monitor.

8 Really cloud-enable the OS

I really like Windows 8's SkyDrive integration, but I think it could go further. Allowing your desktop and profile to travel with you to multiple devices in the style of Live Mesh, or maybe integrating backup for your system and documents without needing to buy something extra, would make the cloud more convenient and practical for desktop users.

9 Buy Stardock

Stardock's Start8 provides a replacement Start menu, whereas ModernMix allows you to run Windows 8 apps in windows on the desktop. Microsoft should just save itself the effort, buy Stardock, and include the company's software in the next release of Windows 8.

10 Rename Windows RT

Every non-IT person I talk to about Windows RT doesn't understand it's not compatible with all the existing Windows x86 software. When I tell them, they can't believe it. The ARM-based Windows RT is a cool device, but giving it a new name would eliminate the confusion. ■

Attention, IT Pros: You Can Help Evolve a Secure Cloud, Too

Driving standards adoption toward a secure web services world

I was at Microsoft in mid-May for meetings on what the company calls its Cloud OS, the holistic combination of Windows Server 2012, System Center 2012, and Windows Azure. Central to the core of this service—or any modern and complex hybrid computing service—is an integrated identity system. But unlike the world of domains and Kerberos, cloud identity protocols and standards are still far from settled.

This predicament is often highlighted (or instigated) by analysts specializing in identity. Last summer at the Cloud Identity Summit, Kuppinger Cole analyst Craig Burton declared, "SAML is dead." Security Assertion Markup Language (SAML) is a widely adopted identity standard, and it's the cornerstone of claims-based authentication. I wasn't able to attend that conference in Colorado, but I think I heard the reaction from my office in Texas. A few months later, Gartner analyst Ian Glazer started a thoughtful discussion with his "Killing IAM In Order to Save It" post, positing that some drastic changes must be made to move identity and access management (IAM) into the modern age.

The latest instance involved the eXtensible Access Control Markup Language (XACML), an OASIS standard for authorization. If you aren't familiar with XACML, don't be too hard on yourself; it hasn't been as widely adopted as its authors hoped. Forrester analyst Andras Csere,



Sean Deuby

is technical director for *Windows IT Pro* and *SQL Server Pro* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

Email

Twitter

in the role of Monty Python's John Cleese in the group's famous Parrot Shop sketch, declared that the XACML parrot is dead. Csere's death proclamation immediately triggered a number of rebuttals that XACML wasn't dead—it was merely resting. (It's worth noting that most of these responses were made by XACML committee members.)

I'm not going to enter the debate over XACML's veracity as the predominant authorization protocol, or whether SAML has seen better days. My point is that, like so many aspects of cloud computing, the core identity protocols that are critical to the success of all other aspects of this computing transformation are still very much evolving. Outside the enterprise, it's an alphabet soup of cloud identity standards and common practices. These standards are each in various degrees of ratification, and versions, and adoption. Kerberos is solid, but from a previous generation, XACML is perhaps looking a bit lost, System for Cross-domain Identity Management (SCIM) is growing healthily, and OAuth 2.0 and its little brother OpenID Connect are booming in popularity. And old-fashioned directory synchronization and the CSV text file aren't going away any time soon.

If cloud computing services ever hope to earn the same trustworthy status as on-premises applications, the identity community must settle on an adoptable set of standards for all aspects of IAM that work equally well on premises and in the cloud. And all these standards must work to get rid of as many passwords as possible. It's exciting but exhausting to keep track of all this; in upcoming columns, I'm going to attempt to make sense of it from an IT pro's perspective. The reality is, however, that the IT pro simply wants products that use standards to interoperate with one another and users as simply and securely as possible.

As IT pros, you must help encourage your vendors to adopt these standards; you're the ones with the checkbooks that they pay attention to. And the end users? Well, they *really* don't care about identity management. They just want to get to their stuff—without having to remember all these stupid user IDs and passwords. ■



Understanding Microsoft System Center 2012 Licensing

In the case of System Center 2012, change is good!

Licensing is never a popular topic. But for most organizations, it's a crucial one. And with System Center 2012, Microsoft has completely changed how System Center is licensed for the management server, managed servers, desktops, and other hardware on the network. The change is definitely for the better; Microsoft has reduced the number of SKUs—the license types an organization can buy—for managed servers from more than 30 to just 2. This huge cut is in large part because of the merging of formerly separate products into the System Center 2012 product.

What's in System Center 2012?

Prior to System Center 2012, System Center was not a product but was instead a family or suite that contained separately purchasable products. These products could also be bought in various combinations, which is why there were more than 30 different ways to buy and license System Center. With System Center 2012, all these products, along with some brand new ones, are now components of a single product. So, which components make up System Center 2012?



John Savill

is a Windows technical specialist, an 11-time MVP, and an MCSE for Private Cloud and Server Infrastructure 2012. He's a senior contributing editor to *Windows IT Pro* and his latest book is *Microsoft Virtualization Secrets* (Wiley).

- System Center 2012 Configuration Manager—The former version of Configuration Manager was System Center Configuration Manager (SCCM) 2007, and Systems Management Server (SMS) before that. Configuration Manager provides capabilities such as OS, application, and patch deployment; hardware and software inventory; troubleshooting tools; and configuration management. System Center 2012 SP1 adds support for Windows 8 and Windows Server 2012, as well as integration with Windows Intune to support single-pane-of-glass management for mobile OSs such as Apple iOS, Google Android, and Windows Phone 8.
- System Center 2012 Virtual Machine Manager—Virtual Machine Manager provides virtual machine (VM) management for Hyper-V, VMware ESX, and Citrix XenServer environments in addition to host management for Hyper-V installations. System Center 2012 adds support for storage and network fabric management and for the concept of the cloud as the primary building block of a Microsoft private cloud solution.
- System Center 2012 App Controller—App Controller is a new component in System Center 2012. It provides a Microsoft Silverlight web portal for end users to create and manage VMs provided by Virtual Machine Manager. With System Center 2012 SP1, App Controller also enables the creation and management of Windows Azure–based services and hosters that leverage the Service Provider Framework (SPF).
- System Center 2012 Operations Manager—You might know Operations Manager under the name of its earliest version, Microsoft Operations Manager (MOM). Operations Manager provides monitoring capabilities to many data center systems, including non-Microsoft systems, network equipment, and custom applications.
- System Center 2012 Data Protection Manager—Data Protection Manager is a best-of-breed backup, continuous data protection, and recovery solution for Microsoft products including SQL

Server, SharePoint, Hyper-V, and desktop computers. One differentiator of Data Protection Manager over many other backup solutions is its powerful recovery features, which include end-user self-service recovery, where appropriate.

- System Center 2012 Service Manager—A configuration management database (CMDB) that includes information from the other System Center components, Service Manager provides a single "point of truth" about assets in your company. It also provides a central service catalog that can utilize all the other System Center components to deliver services. Service Manager also adheres to many IT Infrastructure Library (ITIL) principles and allows creation of incidents, change requests, problems, and so on.
- System Center 2012 Orchestrator—Another new component, Orchestrator (formally the Opalis product, acquired by Microsoft) has connectivity capability to almost any IT system and the ability to perform actions on those systems. By combining the actions into a sequence, runbooks are created. These runbooks can then be executed to automate entire processes and can be used by other systems, including Service Manager.

It's important to note that although System Center 2012 is one product, the components that it comprises are still installed separately on separate OS instances and have separate agents for managed OSs. The Unified Installer component in System Center 2012 RTM performed all the installs for you but was only for simple, proof-of-concept environments and was dropped in System Center 2012 SP1.

With all these components brought together into one product, System Center 2012 now provides heterogeneous management for the entire data center, desktops, physical systems, virtual systems, Windows, Linux, Mac, and much more. These products all integrate tightly with one another for many capabilities, which is why Microsoft took the step to combine them. So how do we buy it?

Licensing Management Servers

The easiest part is licensing the management servers that run the various components and provide the System Center services to managed clients. In the past, a license needed to be purchased for the management servers, but that is no longer the case. Management Server licenses have been effectively discontinued. You can deploy as many management servers as you need to run any of the System Center components to support your deployed, licensed, managed OS instances. There is no System Center cost for the management servers themselves, so you can architect the correct System Center management server layout to provide the optimal environment, without worrying about management server licensing costs.

Every System Center component uses SQL Server in some way to store information such as configuration and historical data. System Center 2012 includes license rights to deploy SQL Server Standard for the sole purpose of supporting System Center 2012, so there are no additional SQL Server license costs, either. Note that if you want to use the SQL Server instances for other uses beyond System Center, you will need to license SQL Server in the typical way. The included license covers only use by System Center and only SQL Server Standard.

Licensing Managed Servers

Now we get to the real licensing consideration: licensing of the server OSs being managed by the various System Center components. If you are familiar with Windows Server 2012 licensing, then you'll understand System Center 2012 licensing. As I previously mentioned, there are now only two System Center 2012 types of license for server OSs: System Center 2012 Standard and System Center 2012 Datacenter. Both types of license cover two physical processors and both have the same features.

So what's the difference? System Center 2012 Standard includes management rights for up to two virtual instances (i.e., server OSs running in a VM, also called Operating System Environments—OSEs).

System Center 2012 Datacenter includes management rights for an unlimited number of virtual instances. With this license, you can use all the various capabilities of the System Center 2012 components on the covered OS instances. You'll typically purchase System Center 2012 Standard for a physically deployed OS (i.e., one that does not use virtualization) or perhaps very light virtualization, in which you have only a couple VMs (maybe in a branch office). System Center 2012 Datacenter is used for virtualized environments and covers all the VMs and the hypervisor host itself.

Remember that each license covers two physical processors, so if a server has four processors, then two copies of System Center 2012 Standard or Datacenter will be required to cover all processors in the server. (Yes, you have to cover all the processors in a server.)

It is possible to "stack" System Center 2012 Standard licenses. For example, if I had a two-processor server and wanted to cover four VMs, I could buy two licenses for System Center 2012 Standard, which gives me four virtual instance rights (each Standard license covers two virtual instances). As the number of VMs increases, the Datacenter license becomes more cost efficient. You can't move System Center 2012 Standard virtual instance rights between servers more frequently than every 90 days, so if you want to cluster servers and use live migration technologies, the Standard license is unlikely to be a good fit.

Notice that I say server OSs and not Windows Server instances. System Center 2012 provides a lot of features for non-Windows server OSs, so you might also want to cover Linux servers, for example. The licensing would be the same. For a physical Linux server, you would buy a System Center 2012 Standard license; a VM would then count as a virtual instance for Standard or Datacenter. Any server OS that is managed by System Center 2012 must be licensed and managed for any communication of data between System Center 2012 and the OS, for the purpose of discovery, configuration, or control of actions.

The public cloud introduces a new licensing consideration. What if you have VMs running in the public cloud (i.e., on Windows Azure

or Amazon Elastic Compute Cloud—EC2) and you want to manage them by using System Center 2012? A single System Center 2012 Standard license covers two virtual OSEs running in the public cloud. You cannot, however, buy one System Center 2012 Datacenter license and cover every VM that you have in the public cloud. That arrangement wouldn't be viable for Microsoft, and since there are no physical processors visible in the public cloud, a Datacenter license covers eight virtual OSEs hosted in the public cloud. Therefore, if you wanted to manage 100 VMs in the public cloud, you'd need to buy 13 System Center 2012 Datacenter licenses.

So far, the licensing choices seem obvious. However, there are a few scenarios in which the licensing requirements might be less apparent.

First, consider System Center 2012 Orchestrator, which can connect to and perform actions on almost any IT system. Those actions might actually instruct that system to perform other actions on still *other* systems to which it is connected. So in effect, Orchestrator provides indirect management of those servers as well. The server OSs that Orchestrator indirectly manages must also be licensed for System Center 2012, even though Orchestrator does not communicate with them directly.

The second component to consider is System Center 2012 Service Manager—specifically, server instances that are not managed by any other System Center 2012 component. Service Manager contains the organization's CMDB, and users and administrators might raise incidents about systems. If the managed system or product is present in the CMDB and has an OSE, then it needs to be licensed for System Center 2012. If the product is not in the CMDB or does not have an OSE, then no System Center 2012 license is required.

Note that a license is *not* required in the following conditions:

- The OSE has no software instances running on it.
- The device functions as a network infrastructure device only (basically, OSI layer 3 or lower).
- The device performs out-of-band (OOB) management only.

If you are unsure about a particular product or configuration in your environment, the best option is to contact your license reseller or Microsoft directly. Things can get a little muddy when it comes to infrastructure components.

Licensing Desktops

Although System Center 2012 can primarily be thought of as a server-management solution, the reality is that it also provides a lot of functionality for desktop OSs, particularly from components such as Configuration Manager, Data Protection Manager, and Service Manager. Three types of System Center 2012 desktop license cover different components of System Center 2012. Which licenses you need depends on which System Center 2012 components the desktops are using. Note that the following licenses are not cumulative in any way, so you might need to purchase all three licenses for a given set of desktops.

- System Center 2012 Configuration Manager Client Management License (ML)—As the name suggests, the Configuration Manager Client ML allows the covered desktop to be managed by Configuration Manager. This management includes deployment of the OS, deployment of applications, patching, inventory, and so on. It also includes Virtual Machine Manager management. This might seem an odd mixture, but consider a Virtual Desktop Infrastructure (VDI) environment that comprises desktop OSs running in VMs. Most likely, these VMs would be managed by Virtual Machine Manager in addition to Configuration Manager, hence the former's inclusion.
- System Center 2012 Endpoint Protection subscription—Configuration Manager includes powerful malware-protection technologies that were previously part of the Microsoft Forefront security family. Endpoint protection is available not only for Windows OSs but also for Linux, UNIX, and Mac OS. Any system that utilizes System Center Endpoint Protection requires this subscription. Note that the System Center 2012 Configuration Manager Client ML does not include this subscription. So if a desktop is being managed by

Configuration Manager and utilizes Endpoint Protection, then both licenses are required.

- System Center 2012 Client Management Suite Client ML—This Client ML allows the covered desktop to be managed by Data Protection Manager, Operations Manager, Orchestrator, and Service Manager.

The System Center 2012 desktop licenses are included with some of the other desktop CALs, which will likely be a common way that organizations acquire System Center 2012 capabilities for desktop OSs that also use other Microsoft technologies. The Core CAL for desktop includes both the System Center 2012 Configuration Manager Client ML and System Center 2012 Endpoint Protection subscription. The Enterprise CAL for desktop includes all three System Center 2012 desktop licenses.

Simpler Licensing

With a few minor exceptions, the licensing for System Center 2012 is far simpler than in the past. However, for organizations to get real value for the new single-product license, it's crucial that multiple, if not all, components are deployed and used, which is what Microsoft intends with this merged product. If the integration between the components is explored, especially through Service Manager and Orchestrator, the most functional deployment is one in which all the components are deployed and linked together. And with the new licensing, if you own one component you own them all!

For organizations that previously owned licenses for individual products that were covered by Software Assurance (SA), Microsoft offers a grant that converts the individual product licenses to a new System Center 2012 license. Make sure your organization has taken advantage of that, and talk to your license reseller if you need more information. ■

Enable Claims Support in Windows Server 2012 Active Directory

Creating claims in Active Directory isn't hard, but understanding how to use them can be difficult

One new, lesser-known feature in Windows Server 2012 Active Directory Domain Services (AD DS) is support for claims-based authentication. This lack of prominence belies the feature's significance to the future of Active Directory (AD) and AD's interaction with the enormous world of web services.

Claims aren't new; they've been around in one form or another almost as long as computers. In its simplest form, a claim is a statement made by a party. That's all. It's a bit more complicated than that, of course, but that's the core concept. The power of claims-based identity is that a party (also known as the identity provider; for example, a company) makes an assertion that its user Jim Bob is a member of the engineering department. The web service (also known as the relying party or service provider, such as a Software as a Service—SaaS—application) that wants to use this bit of identity data trusts the digitally signed information coming from the company.

And—this is important—the process doesn't need Jim Bob's password to accept the assertion. You can stop practically anyone on the street today, and that person would tell you in so many words that password-based authentication has outlived its usefulness. It's critical that companies move to authentication and authorization methods that don't require passwords. Claims-based authentication is at the core of federated identity, and through federation you can securely



Sean Deuby

is technical director for *Windows IT Pro* and *SQL Server Pro* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

Email

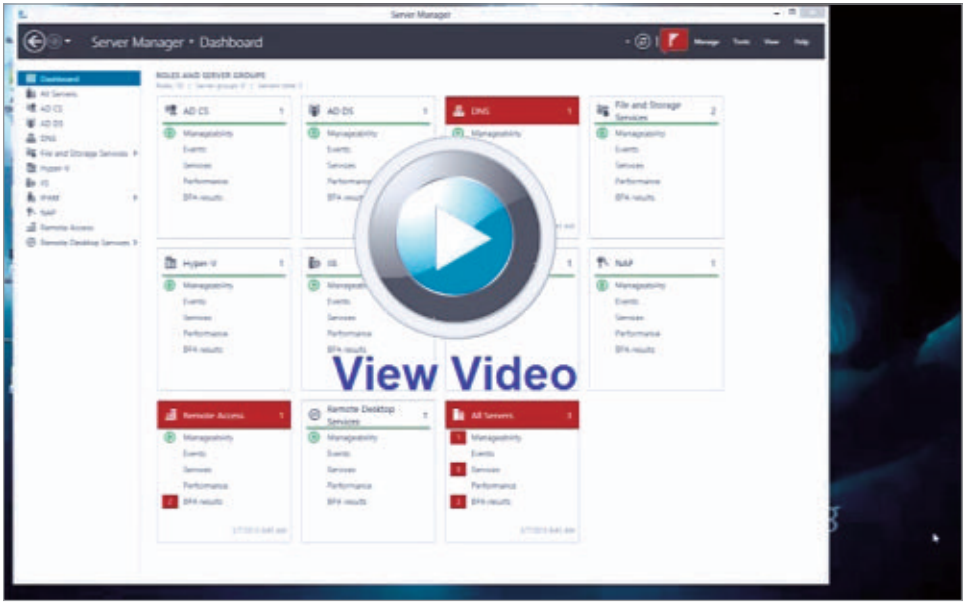
Twitter

extend your corporate identity to access web services for which you'd otherwise have to create a user ID and password.

Claims made their first foray into Windows with Active Directory Federation Services (ADFS), a connector to the external web services world. Before Server 2012, ADFS created claims from AD security groups and LDAP queries that it made to AD. In Server 2012, ADFS 2.1 consumes claims directly from AD. Early in the life of ADFS I described it as a technology without a business need because there was little need for claims-based authentication in the Windows world. The rise of cloud services, and SaaS in particular, however, has changed that. Federation services, whether on premises like ADFS or hosted in the cloud as an identity management as a service solution, provide a gateway between the Kerberos-based world of AD and the claims-based world of web services.

Video

Enabling claims in Windows Server 2012 Active Directory using the Group Policy Management Console and Active Directory Administrative Center



Claims have made their entrance into AD specifically to support Dynamic Access Control and conditional expressions in file services ACLs. And as I said, claims also are consumed by ADFS 2.1. So if

you're interested in implementing Dynamic Access Control, ADFS 2.1, or conditional expressions to control access to data on Windows file servers, you need to implement AD claims. Server 2012 AD supports both user claims and device claims.

Understand Active Directory Claims Architecture

The schema update for Active Directory in Server 2012 introduces several new class objects:

- msDS-ValueType
- msDS-ClaimTypePropertyBase
- msDS-ClaimType
- msDS-ResourceProperty
- msDS-ResourcePropertyList
- msDS-ClaimsTransformationPolicyType

The central access policies (and their constituent rules) that Dynamic Access Control uses are supported by the following class objects:

- msAuthz-CentralAccessRule
- msAuthz-CentralAccessPolicy

Claims created in AD are stored in the Configuration partition, under CN = Services,CN = Claims Configuration (Figure 1).

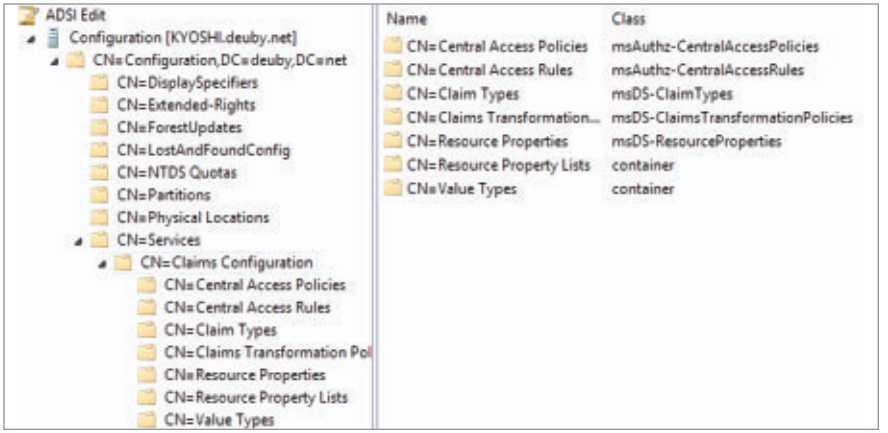


Figure 1
Claims Created in Active Directory Are Stored in the Configuration Partition

How do these claims make it from AD to the client? The answer is Kerberos, the standard authentication and authorization protocol used by Windows. Kerberos is by far the most logical place to insert claims; otherwise, a second security protocol would have to be designed within the Windows security system—no small task.

If you're familiar with the Kerberos protocol, you recognize that the only place you can put such data (i.e., claims) is in the Privilege Account Certificate. The PAC is an extension element of the authorization-data field contained in the client's Kerberos ticket-granting ticket (TGT). The PAC structure conveys authorization data provided by domain controllers (DCs) to Windows clients. Before Server 2012, the PAC contained information such as SIDs, group membership (also in a SID format), user profile information, and password credentials.

In Server 2012, the Kerberos PAC contains the previously mentioned security information plus user and device claims. If you've been concerned about Kerberos token bloat in your environment, then you're probably thinking, "Microsoft is cramming *more* data into the PAC while large companies are already running into PAC storage limitations?" Microsoft has addressed this concern in several ways, which supposedly mitigate the problem. First, MaxTokenSize (the amount of buffer allocated to store authorization information) has been bumped from 12KB in previous versions to 48KB in Server 2012, which helps eliminate authorization failures in applications such as Microsoft IIS. There's also a Group Policy setting that warns of large Kerberos tickets.

Finally, Server 2012 has introduced SID compression, a BFO (blinding flash of the obvious) enhancement that saves PAC space. I'll describe SID compression in more detail in an upcoming article.

Why aren't *all* AD attributes automatically representable by claims? The simplest explanation is that making every populated attribute of the user or device object available as a claim would include these claims in the Kerberos PAC no matter whether they are used. And most *won't* be used, so it would be a massive and unnecessary increase in data overhead in an area that doesn't have a lot of it to spare. It's a much

cleaner solution to determine which attributes you need to make available as claims based on your conditional expressions and Dynamic Access Control requirements and then create claim types for them.

Windows Server 2012 File and Storage Services is the only server role that uses claims-based access control in this first implementation of the technology, although I'm sure other roles will pick up claims-based access control in future versions of the OS. Though of less interest to server administrators, Windows 8 also takes advantage of claims-based access control (which I discuss in the following section).

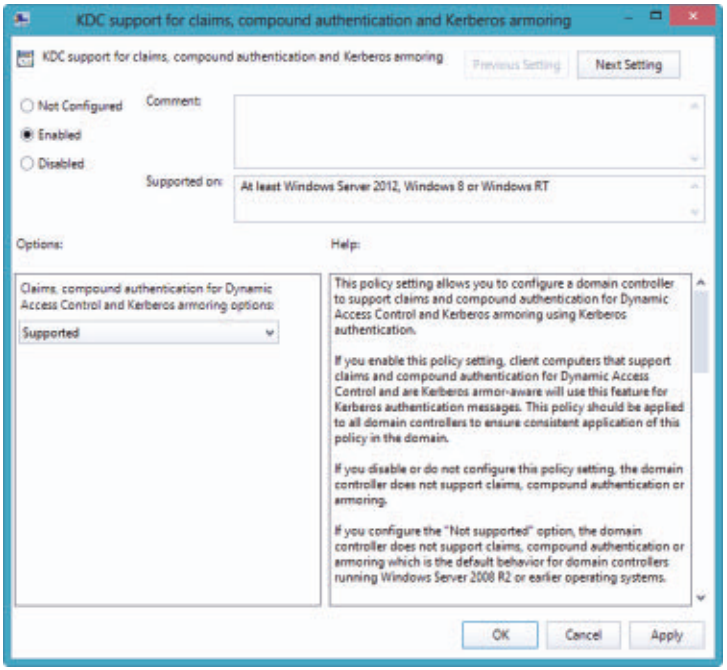
Implement Claims

You must perform several steps to enable claims in Server 2012 AD. First, you must upgrade the forest schema to Server 2012. You can do so manually through Adprep, but Microsoft strongly recommends that you add the AD DS role to a new Server 2012 server or upgrade an existing DC to Server 2012. This process automatically performs all required Adprep operations (see "Windows Server 2012 Simplifies Active Directory Upgrades and Deployments").

Once AD can support claims, you must enable them through Group Policy:

1. From the Start screen on a system with AD admin rights, open Group Policy Management and select the Domain Controllers Organizational Unit (OU) in the domain in which you wish to enable claims.
2. Right-click the Default Domain Controllers Policy and select Edit.
3. In the Editor window, drill down to Computer Configuration, Policies, Administrative Templates, System, and KDC (Key Distribution Center).
4. Open *KDC support for claims, compound authentication, and Kerberos armoring.*
5. Select the Enabled radio button. *Supported* will appear under *Claims, compound authentication for Dynamic Access Control and Kerberos armoring options* (Figure 2).

Figure 2
Enabling Claims Through Active Directory Group Policy



Note that there are four settings for this policy, in order of increasing control: Not Supported, Supported, Always Provide Claims, and Fail unarmored authentication requests. I recommend that you study "Dynamic Access Control: Scenario Overview" before configuring this policy.

Once the policy is enabled and has replicated to all Server 2012 DCs in the domain, you must create claim types. To do this, launch Active Directory Administrative Center, which you can see in Figure 3.

Although it's similar to Active Directory Users and Computers, the Active Directory Administrative Center also has an item for Dynamic Access Control (in addition to the deuby domain) on the left side of the navigation pane. Select Dynamic Access Control and then Claim Types to bring up AD claim types.

Figure 4 shows two claim types that I created previously. Selecting New from the task pane on the right brings up the Create Claim Type dialog box, which you can see in Figure 5.

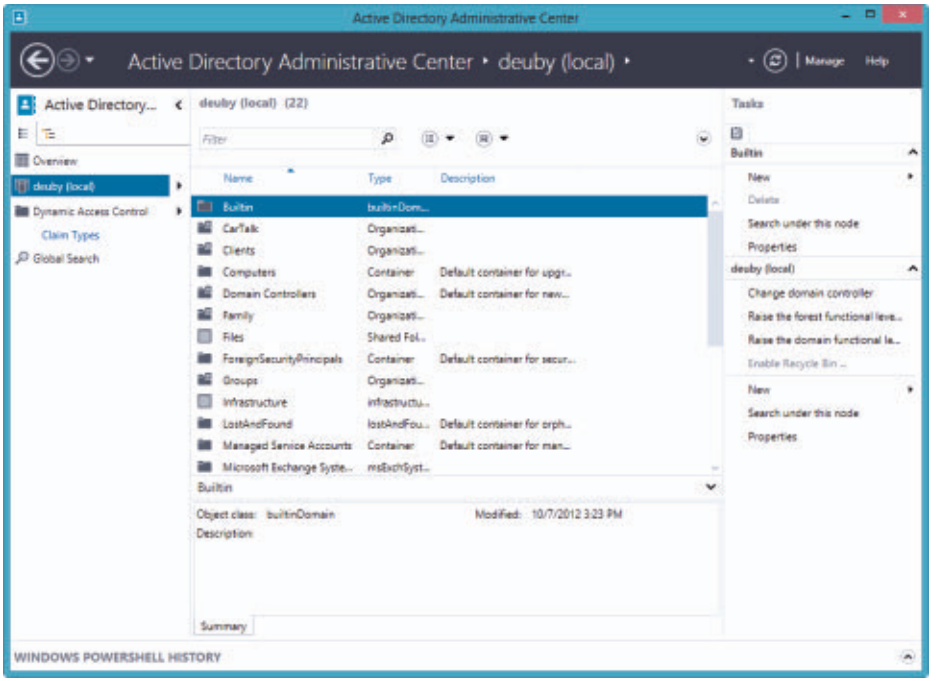


Figure 3
Active Directory Administrative Center

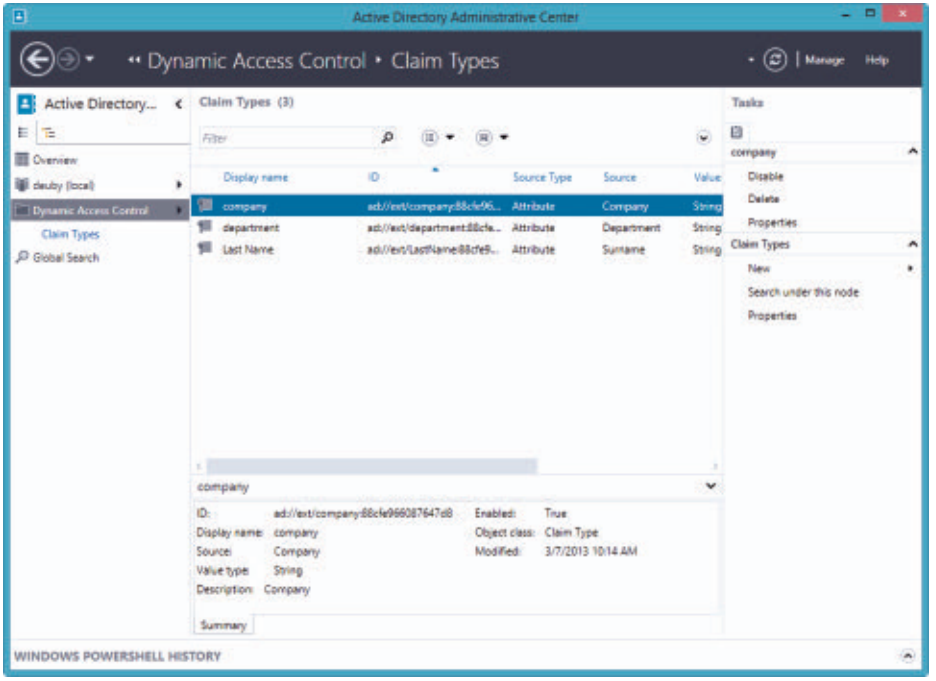
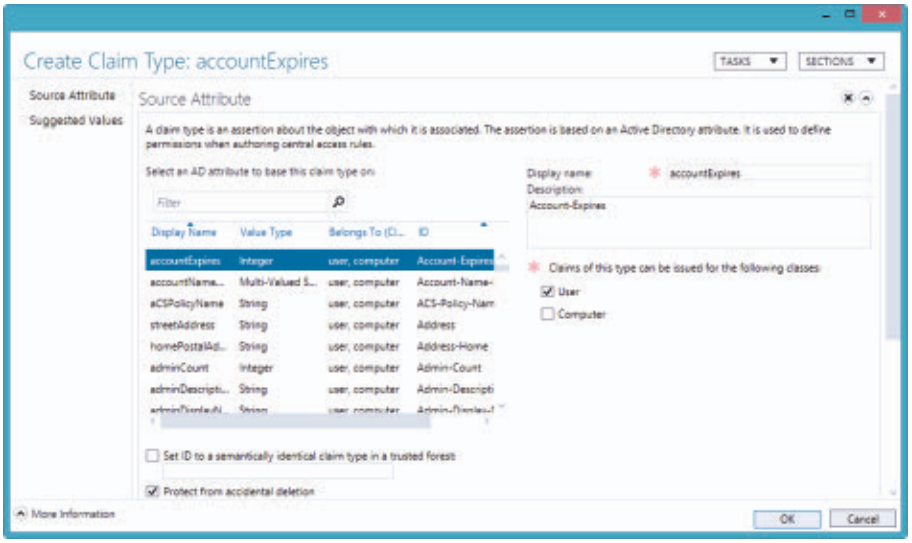


Figure 4
Active Directory Claim Types

Figure 5
Create Claim Type Dialog Box



The Source Attribute section displays a list of attributes that can be represented by claims. Windows creates the list of attributes from the following schema class objects:

- User
- InetOrgPerson
- Computer
- ManagedServiceAccount
- GroupManagedServiceAccount

By default, the Create Claim Type dialog box shows the accountExpires attribute because it's the first attribute on the list. Display name and Description are shown on the right; this is where you can change these fields to something more descriptive. For example, I can create a third claim type associated with the user's last name. The AD attribute ID for one's last name is surname, with a display name of sn. Entering surname in the *filter* field brings up this attribute (Figure 6). For this example I changed the display name of the claim type to something more useful: Last Name. Selecting OK brings up the Active Directory Administrative Center dialog box showing the newly created claim type (Figure 7).

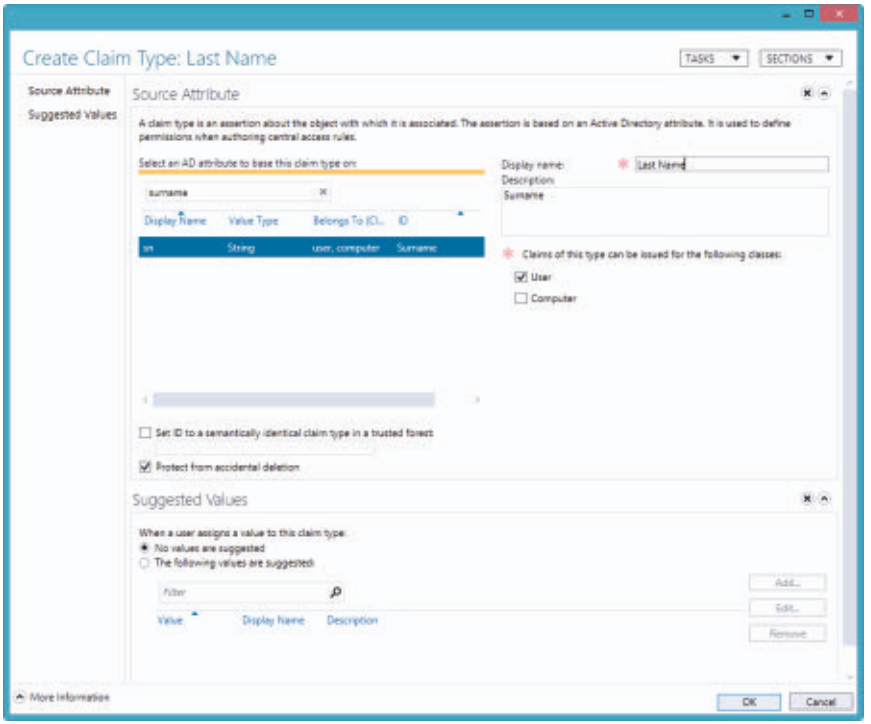


Figure 6
Creating a Claim Type Associated with the User's Last Name

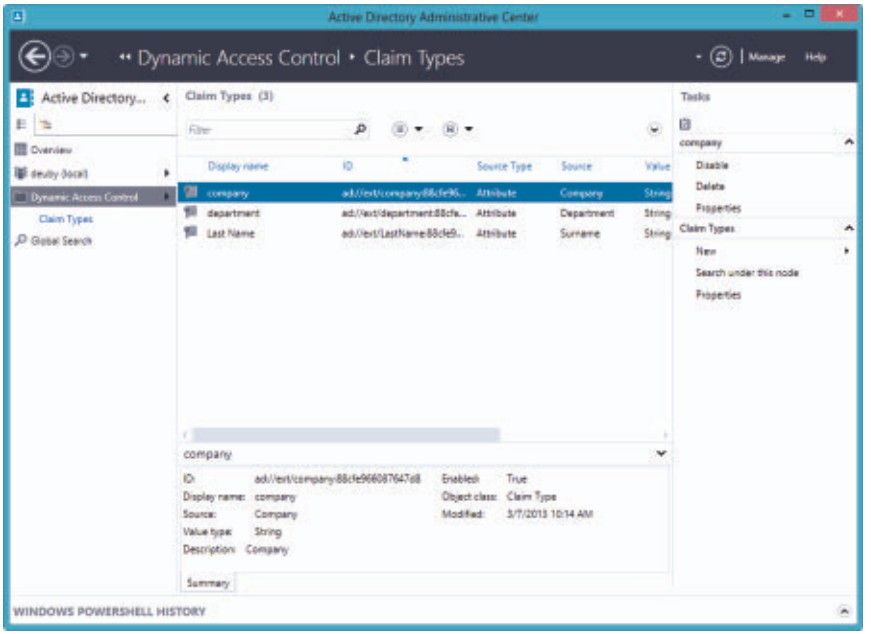


Figure 7
Active Directory Administrative Center Showing Claim Type Last Name

As I alluded to, you can use conditional expressions with claims in both Server 2012 and Windows 8 to provide a fine degree of access control to file folders. Figure 8 shows how the claim types I created can be used in an advanced security dialog box to modify access to config.bgi based on company, department, or last name (in addition to group membership). This demonstrates how Server 2012 can control access to files and folders based directly on AD attributes.

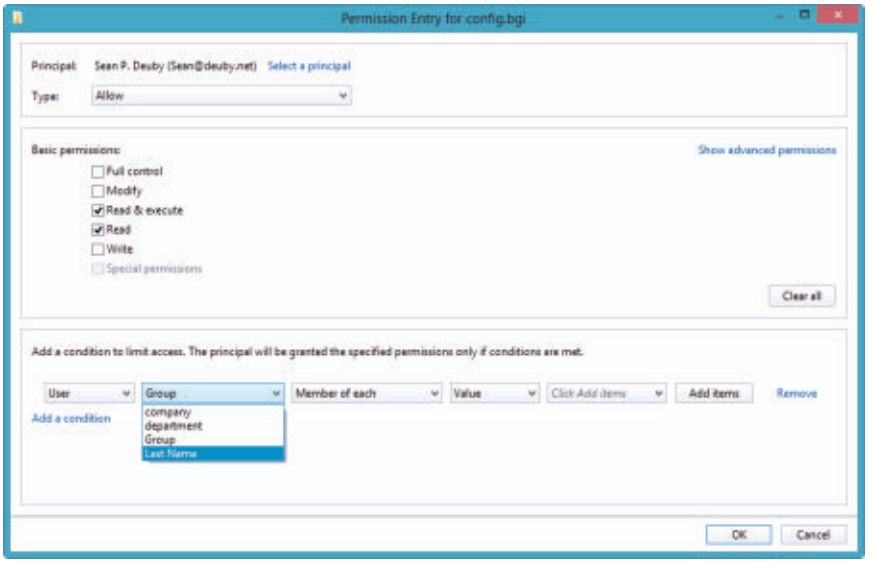


Figure 8
Using Claim Types to Control Access to Files and Folders

Use Claims-Based Authentication

Claims are an unheralded AD DS feature in Server 2012. They're an integral component of Dynamic Access Control, but you can take advantage of them to simplify Windows file server access control without implementing Dynamic Access Control at all. I'll demonstrate the basics of this claims-based access control in an upcoming article. ■

Integrating Hyper-V and vSphere Management

Manage a multi-hypervisor environment from a single management console



Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro*.

Email

While VMware is the clear leader in enterprise virtualization, it's also apparent that Microsoft Hyper-V is growing quickly. The Windows Server 2012 release of Hyper-V brought its A-game to scalability, putting it on par with VMware's vSphere. The fact that Hyper-V is bundled with more recent versions of Windows Server makes it especially appealing to small-to-midsized businesses (SMBs) and is definitely driving Hyper-V's growth in the SMB space. A Gartner Research study showed that Hyper-V had an 85 percent share of the market of organizations with fewer than 1,000 employees. The rapid growth of Hyper-V means that many organizations have both VMware's vSphere and Microsoft Hyper-V deployed.

There are pluses and minuses to having a multi-hypervisor environment. On the plus side, you can use the hypervisor that makes the most sense for your virtualization needs. However, multiple hypervisors also means more complexity, and with different technologies you usually need different skill sets and personnel to manage each of the platforms you implement. This means an organization winds up creating different islands of computing to handle different technologies.

Both Microsoft and VMware have tools that help manage multi-hypervisor environments. In this article, I show how VMware's vCenter Multi-Hypervisor Manager and Microsoft System Center Virtual Machine Manager (VMM) 2012 let you manage multiple hypervisors from their respective management consoles. For more information about managing a multi-hypervisor environment, see the accompanying video.

Video

Windows Server 2012: Integrating Hyper-V and vSphere management



VMware's vCenter Multi-Hypervisor Manager

VMware's vCenter Multi-Hypervisor Manager enables you to manage Microsoft Hyper-V servers and their virtual machines (VMs) from the vSphere Virtual Infrastructure Client (also known as the vSphere Client). The Multi-Hypervisor Manager has a client and server component. The server component is installed on your VMware vCenter server, whereas the client component is installed on your VMware Virtual Infrastructure Client. If you've been keeping up with VMware, then you know that with vSphere 5.1, VMware stated that the desktop-based vSphere Client would be deprecated, and all future enhancements would be made to the new vSphere Web Client. Even so, the new Multi-Hypervisor Manager only works with the Windows-based vSphere Virtual Infrastructure Client. I would expect support for the vSphere Web Client in the future.

VMware's Multi-Hypervisor Manager has several requirements. First, you must be running vSphere 5.1 Standard edition or higher and have a vCenter Server system installed. The Multi-Hypervisor Manager doesn't work with the vSphere Essentials edition. In addition, it

can connect only to Windows Server 2008 R2, Windows Server 2008, Hyper-V Server 2008 R2, or Hyper-V Server 2008. Notably, the current Multi-Hypervisor Manager 1.0 release can't connect to Windows Server 2012 Hyper-V or Hyper-V Server 2012. That will undoubtedly change in the near future.

There is a server portion of the Multi-Hypervisor Manager that installs on the vCenter server. You also need to install a client portion on the systems running the vSphere Virtual Infrastructure Client that you intend to use to manage Hyper-V. You can download both of these pieces with VMware's vCenter components. The current server component is called VMware-MHM-5.1.0-901315.exe and the vSphere Infrastructure Client plug-in is called VMware-MHM-Client110912.exe.

The Multi-Hypervisor Manager server component requires an x64 server with an additional 2GB of RAM on top of the vCenter Server requirements. This server portion communicates with the Microsoft Hyper-V servers. In addition, the Windows Remote Management service must be running on the vCenter server.

Installing the vSphere Virtual Infrastructure Client plug-in was a simple task that took only a few seconds to click through the wizard. Afterward, the vSphere Virtual Infrastructure Client needs to be restarted.

Installing the Multi-Hypervisor Manager on the vCenter server was also easy and relatively painless. You need to be logged on with administrative privileges before beginning the installation. The installation wizard opens with a Welcome dialog box and then displays an end-user patent agreement, a license agreement dialog box, and an installation directory dialog box. Clicking through these dialog boxes displays the vCenter Multi-Hypervisor certificate dialog box. You have the option of automatically generating a certificate, or you can choose to provide a certificate later. I chose to automatically generate a certificate. The next installation dialog box prompts you for the connection properties of the vCenter server. On that dialog box you need to provide the host name or IP address, accept or change the default TCP ports, and provide the vCenter server's authentication information.

After that, a vCenter Server SSL certificate configuration page appears. You must enter a login that has sufficient rights to run the vCenter Multi-Hypervisor Manager service and has permissions to issue Windows Remote Management commands. Clicking Next and then Install completes the server installation and the vCenter Multi-Hypervisor service is running and ready to connect. Figure 1 shows an overview of VMware's vCenter Multi-Hypervisor Manager architecture.

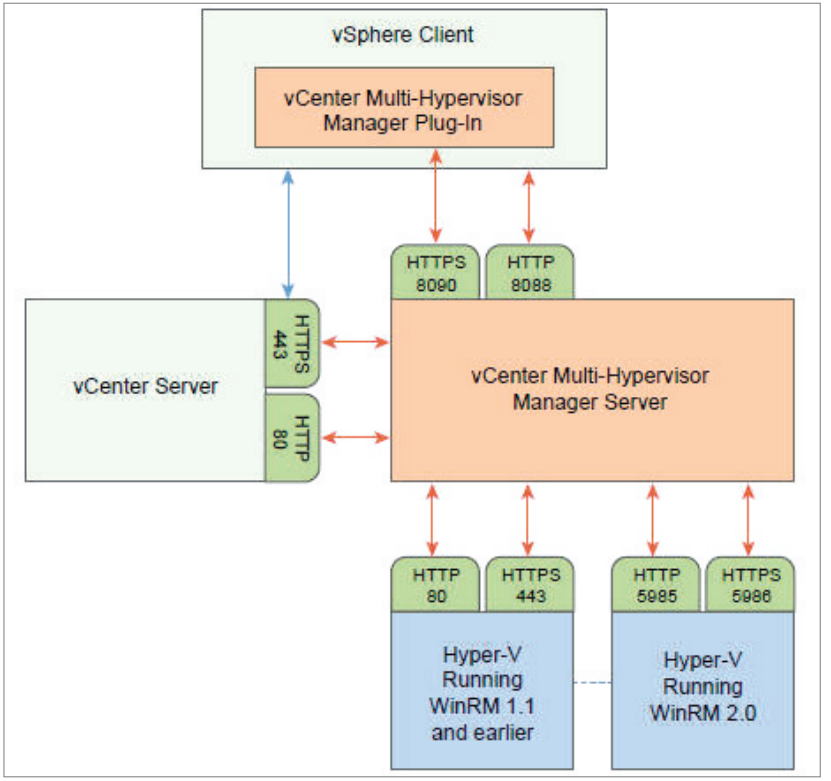


Figure 1
VMware's vCenter Multi-Hypervisor Manager Architecture

You can see the client and server components used by the Multi-Hypervisor Manager. The vSphere Virtual Infrastructure Client uses ports 8090 and 8088 to communicate with the Multi-Hypervisor Manager server, which in turn uses ports 80 and 443 to connect to WinRM 1.1 systems and ports 5985 and 5986 to connect to the Hyper-V servers running WinRM 2.0.

Before configuring the Multi-Hypervisor Manager to connect to a Windows Server Hyper-V system, you must make sure the Windows Server Windows Remote Management (WinRM) Extensions feature is installed. You also need to run the following command on the Server 2008 R2 or Server 2008 system:

```
Winrm quickconfig
```

After configuring WinRM, you need to be sure that the firewall ports shown in Figure 1 are open on the Hyper-V server.

To configure the Multi-Hypervisor Manager, open the vSphere Virtual Infrastructure Client and connect it to the vCenter server where you installed the Multi-Hypervisor Manager. After connecting to the vCenter server, use the top navigation bar to go to Home, Inventory, vCenter Multi-Hypervisor Manager. This opens the Multi-Hypervisor Manager view. Next, click the link *Add a Third Party Host* to start the Add Host Wizard shown in Figure 2.

Add the Hyper-V host connection information on the Connection Settings screen. As Figure 2 shows, you need to specify the host name

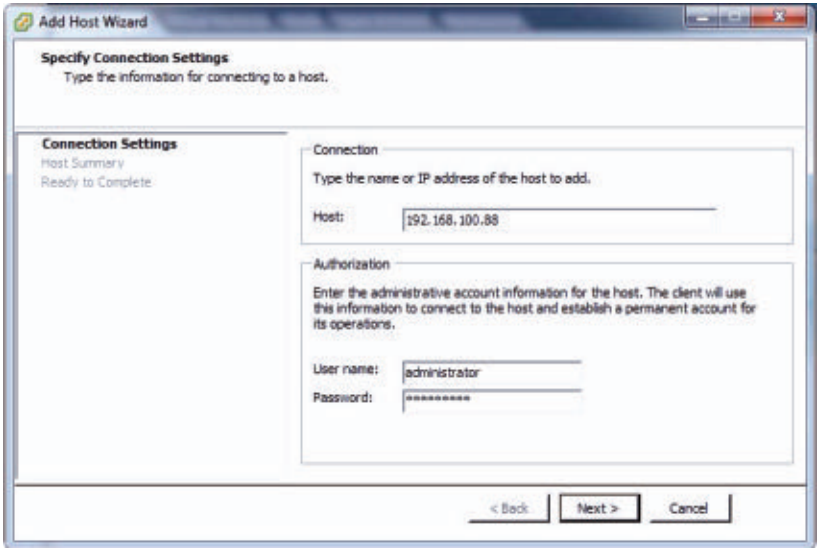
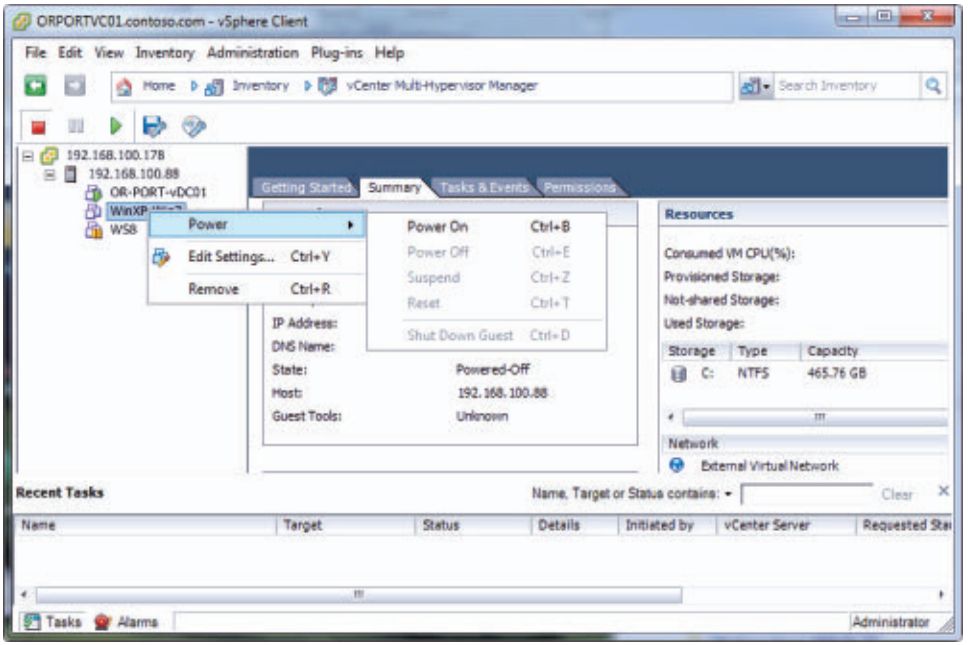


Figure 2
Connecting the Multi-Hypervisor Manager to Hyper-V

or IP address and add the authentication information for the Hyper-V host. I entered the IP address 192.168.100.88, which is the IP address for a specific Windows Server 2008 R2 Hyper-V system. Clicking Next displays a warning dialog box about the connection not being encrypted. In my case, I chose to leave the connection unencrypted and clicked OK to bypass the warning dialog box.

The next screen is the Host Summary. The Host Summary dialog box displays the fully qualified host name, the OS type, and all VMs that are present. Click Next to display the *Ready to Complete* summary dialog box, which essentially lets you confirm your settings. Click the Finish button on the *Ready to Complete* dialog box. When the Add Host Wizard completes, the Hyper-V host and all its VMs are added to the Multi-Hypervisor Manager view (Figure 3).

Figure 3
Using the Multi-Hypervisor Manager



Click the plus sign in front of the Hyper-V host name to expand the host node and see the VMs it contains. Right-clicking any of the VMs displays the context menu shown in Figure 3. The context menu

allows you to perform basic VM management tasks. You can Power On, Power Off, Suspend, and Reset a VM. You also can create new VMs and change a VM's properties, including the number of virtual CPUs or memory or whether the VM is connected to the host's physical DVD drive. The current Multi-Hypervisor Manager 1.0 release doesn't let you perform more advanced operations such as initiating Live Migration. However, if you want to add basic management of Hyper-V VMs to your vSphere Client, then the Multi-Hypervisor Manager fills the bill.

Microsoft Virtual Machine Manager 2012

Microsoft System Center Virtual Machine Manager (VMM) 2012 has the capability to manage multiple hypervisors right out of the box—there's nothing extra to install. VMM 2008 R2 first added support for vSphere to the VMM 2008 release. Table 1 lists the different versions of VMware and vSphere that are supported by the different releases of VMM.

Table 1: VMware and vSphere Versions Supported by Virtual Machine Manager

Virtual Machine Manager (VMM)	VMware/vSphere
VMM 2008 R2	VMware vCenter 2.5, 4.0 ESX 3.5, 4.0
VMM 2012	VMware vCenter Server 4.1 ESXi 4.1, 3.5 ESX 4.1, 3.5 XenServer 6.0
VMM 2012 SP1	VMware vCenter Server 4.1 VMware vCenter Server 5.1 EXSi 5.1, 4.1 ESX 4.1 XenServer 6.0

VMM requires a vCenter server to connect to vSphere. The connection is agentless, so there's nothing to install on the vCenter server itself. VMM connects to the vCenter server using VMware's Infrastructure Web Services, and it can manage multiple vCenter servers.

VMM's vSphere connectivity is in its second release, so it's a more mature product than VMware's Multi-Hypervisor Manager. VMM provides many more advanced capabilities, such as the ability to initiate vMotion and Storage vMotion on the vSphere platform. Some of the latest VMware-related enhancements to VMM 2012 include:

- Doesn't import VMware tree
- Lets you add selected ESX servers and hosts to any VMM host group
- Imports VMware templates
- Supports standard and distributed switches
- Supports less-privileged accounts
- Automates discovery of port groups
- Supports thinly provisioned disks

To connect to vSphere, open VMM and create a Run As account. The Run As account passes authentication information to the vCenter server. The credentials that you specify for the Run As account must have administrative permissions on the vCenter server. Creating the Run As account is optional at this point because you'll be prompted to do so later if you haven't already; but you need a Run As account, and it's a good idea to know where to manage this feature. To create the Run As account, click the Settings link in the VMM console's left pane. Next, click the Create Run As Account option to display the Create Run As Account dialog box. Give the Run As account a descriptive name in the Name prompt and provide an account with administrative rights on the vCenter server. In my example, I named the Run As account vCenter Administrator. You can optionally validate the account's domain credentials, but that's only required if you use a domain account. Click OK to create the Run As account.

Next, add the vCenter server to VMM 2012. First, select the Fabric link in the VMM console. Then right-click the vCenter Server link and select the Add VMware vCenter Server option from the context menu. This displays the Add VMware vCenter Server dialog box shown in Figure 4.

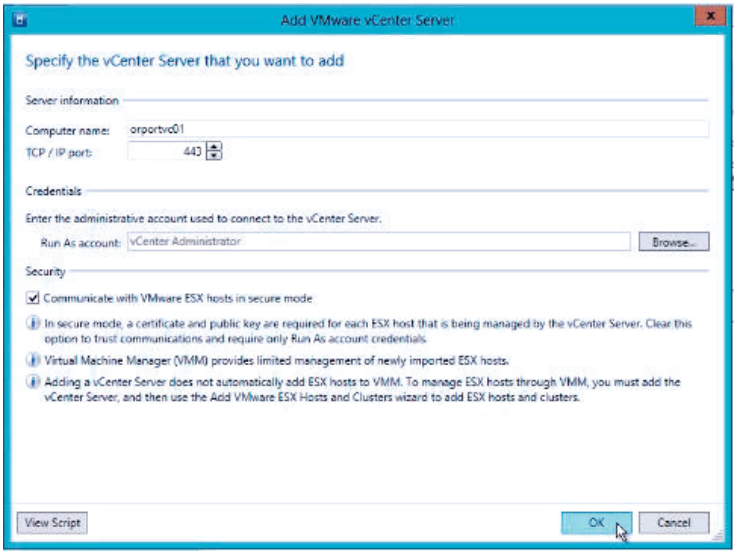


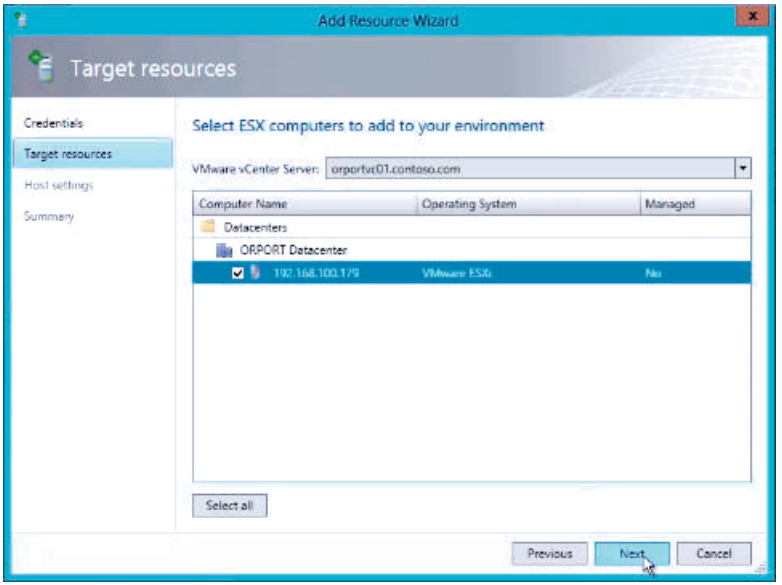
Figure 4
Adding the vCenter Server to the Virtual Machine Manager Fabric

Supply the DNS host name or IP address of the vCenter server in the *Computer name* prompt. TCP/IP port 443 is the default. You can change this if necessary. In my case, I left it at the default value. Next, supply the Run As account that will connect to the vCenter server. I used the vCenter Administrator Run As account that I created earlier (Figure 4). You can optionally clear the *Communicate with VMware ESX hosts in secure mode* check box. I left it checked. Click OK to add the vCenter server to your VMM 2012 fabric.

After you've added the vCenter server to the VMM 2012 fabric, you can add your ESX or ESXi servers to VMM 2012's *VMs and Services* section. First, click the *VMs and Services* entry in the lower left pane. Next, you probably want to create a new host group for your vSphere server, but this is optional. You can add the VMware ESX server to existing groups. In my case, I created a new host group by right-clicking the All Hosts node and then selecting New Host Group from the context menu. I named my new host group VMware vSphere.

Next, right-click the new VMware vSphere host group and select *Add VMware ESX Hosts and Clusters* from the context menu, which starts the Add Resource Wizard. The first dialog box in the Add Resource

Figure 5
Adding an ESXi Server to the Virtual Machine Manager 2012 VMs and Services



Wizard prompts you for the Run As account. Click the Browse button and select the vCenter Administrator account that you created earlier and then click Next to display the *Target resources* dialog box (Figure 5).

The Add Resource Wizard connects to the vCenter server and queries the different hosts that are running. In Figure 5, you can see one ESXi host with the IP address 192.168.100.179. Select the check box to indicate that you want to manage this ESXi host using VMM 2012. Click Next to display the Host Settings dialog box, which lets you change the host group that contains the ESXi server as well as the default storage location that the virtual machine uses. I left all the values on the Host Settings dialog box at their default settings and clicked Next. This displays the *Confirm the settings* dialog box where you can review your ESXi server connection settings and page back through the dialog boxes to make any changes. When everything is the way you want, click Finish to launch VMM 2012's Jobs dialog box, which shows the status of adding the ESX Server hosts. When the Job status reaches 100 percent, the ESXi server will have been successfully added and you can close the Jobs dialog box. When VMM

2012 first connects to the ESX server, it takes it a couple of minutes to retrieve all the VM information from that host. After VMM 2012 has finished retrieving the VM information, all the ESXi VMs and their status will be displayed in the VMM console (Figure 6).

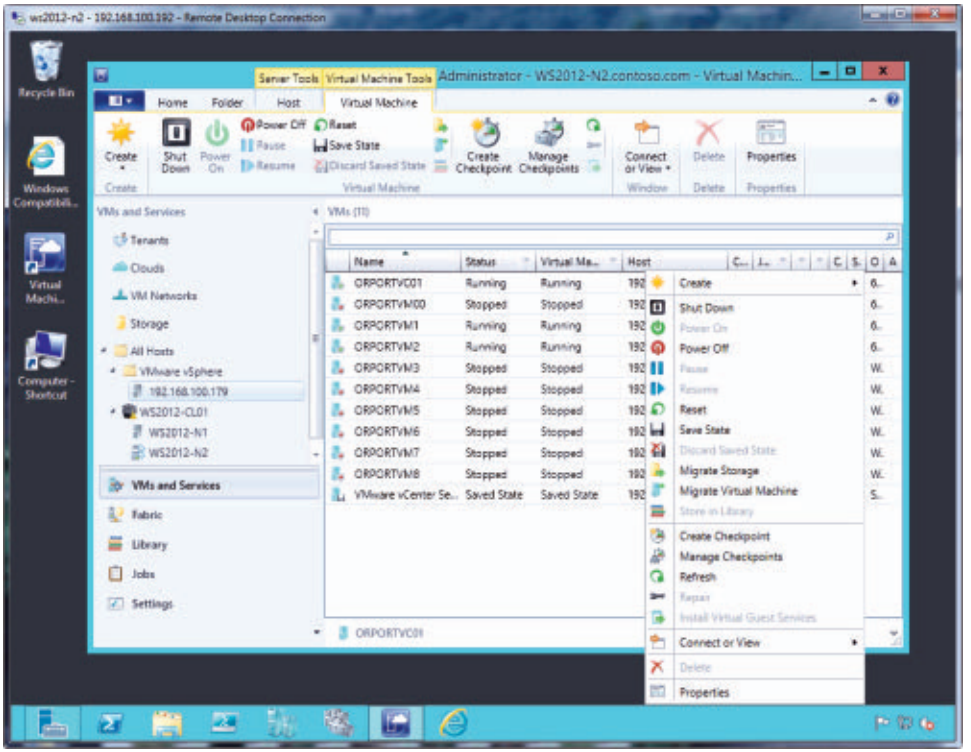


Figure 6
Managing VMware ESXi from Virtual Machine Manager 2012

You manage the vSphere ESXi Server VMs very much like you manage Hyper-V VMs. Right-click an ESXi Server VM to launch the context menu (Figure 6). The context menu shows various management actions that you can take with the VMware VMs. You can create new VMs and modify the properties of existing VMs. You can also perform power management functions such as Power On, Shut Down, Power Off, Pause, and Resume. In addition to these basic functions, VMM 2012 also performs more advanced functions. The Migrate Storage option initiates a Storage vMotion, whereas the Migrate Virtual Machine option initiates a vMotion to move the VM to another ESX server.

The Management Mix

The tool you choose will probably depend on your environment. If you primarily use VMware's vSphere with a dabbling of Hyper-V here and there, then VMware's Multi-Hypervisor Manager makes a lot of sense—especially because it comes with vSphere Enterprise and higher editions at no extra cost. However, it can't perform the more advanced functions such as initiate Live Migrations or Storage Live Migrations. Microsoft System Center VMM 2012 is the more full-featured, multi-hypervisor management solution. And it makes more sense for organizations that primarily use Hyper-V, or if you already have the System Center Suite. However, if you don't have System Center, you have to buy the System Center 2012 Suite to get VMM 2012 and its multi-hypervisor management capabilities. Both solutions can answer your basic, multi-hypervisor management needs, but the best solution depends on your organization's platforms and requirements. ■

Reader to Reader

Allowing a User to Access Another User's Exchange 2003 Mailbox

Sometimes a manager, co-worker, or assistant needs to access another user's mailbox. I'll discuss three recommended methods you can use to achieve this in Microsoft Outlook 2010 and Outlook 2003, and Microsoft Exchange Server 2003. I'll also let you know about some methods to avoid. To demonstrate these methods, let's say that Bob (i.e., user1) needs access to the mailbox of Sally (i.e., user2).



Bret A. Bennett

is the principal consultant of BRET A. BENNETT. He specializes in the installation, training, and support of Microsoft Dynamics GP, Passport Business Solutions, and Open Systems Traverse software, and he provides support for BI delivery and Microsoft servers.

Email

Method 1

One way to give Bob access to Sally's mailbox is to use delegation, which can be achieved without the involvement of an administrator. First, Sally needs to give Bob access to her mailbox. In Outlook 2003, this is done by choosing Options on the Tools menu, selecting the Delegates tab, and clicking the Add button, as shown in Figure 1. (In Outlook 2010, it's done by selecting Info on the File tab, clicking Account Settings, choosing Delegate Access, and clicking Add.) Clicking Add spawns the Add Users dialog box. Sally just needs to highlight Bob's Active Directory (AD) username, click the Add button, and click the OK button. This brings up the Delegate Permissions dialog box shown in Figure 2. In it, Sally can configure the permissions she wants to give Bob for each of the following folders: Calendar, Contacts, Inbox, Journal, Notes, and Tasks.

After Sally has given Bob delegate permissions, Bob can access Sally's mailbox in his Outlook client. To do so, he needs to select Open on the File menu and click the Other User's Folder option. In the dialog box shown in Figure 3, Bob can then click the Name button, select

Figure 1
Adding a Delegate

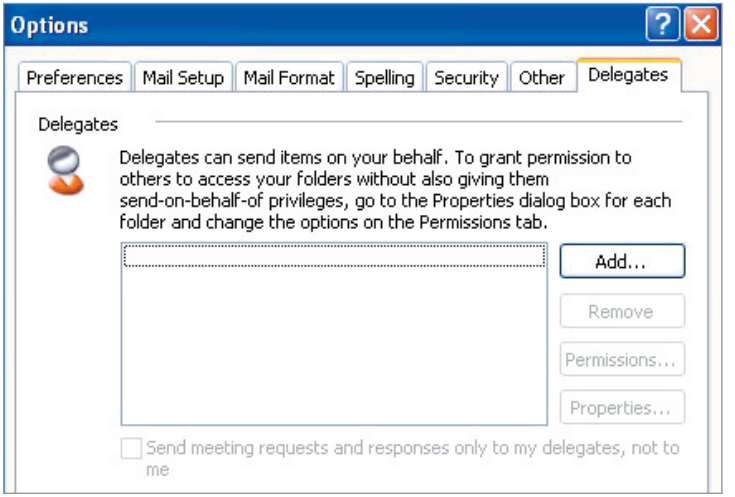


Figure 2
Configuring the Delegate's Permissions

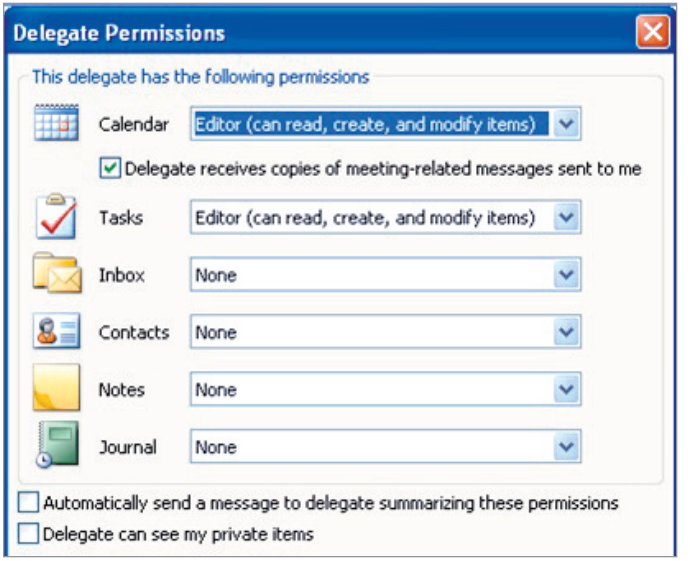
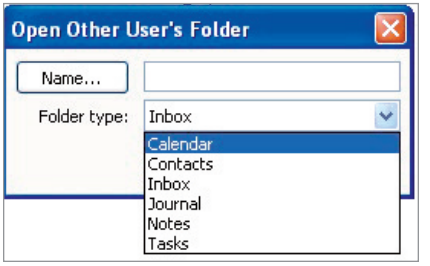


Figure 3
Opening Another User's Folder



Sally's AD username, and select the folder he wants to access.

When Bob replies to Sally's email, the email reply will include "on behalf of" in the From field. Figure 4 shows an example of this.

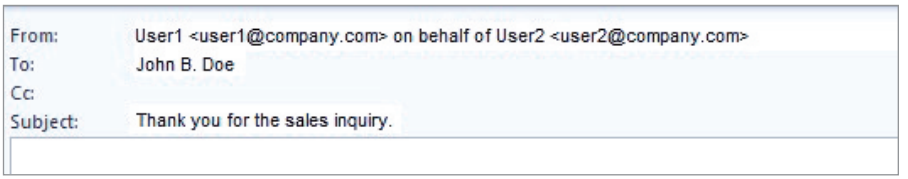


Figure 4
Letting an Email Recipient Know the Message Was Sent on a User's Behalf

The main advantages to Method 1 are that an administrator doesn't need to be involved and users can easily understand what permissions they're giving to other users. The disadvantage is that Bob can access only six folders (i.e., Calendar, Contacts, Inbox, Journal, Notes, and Tasks) and only one folder at a time.

Method 2

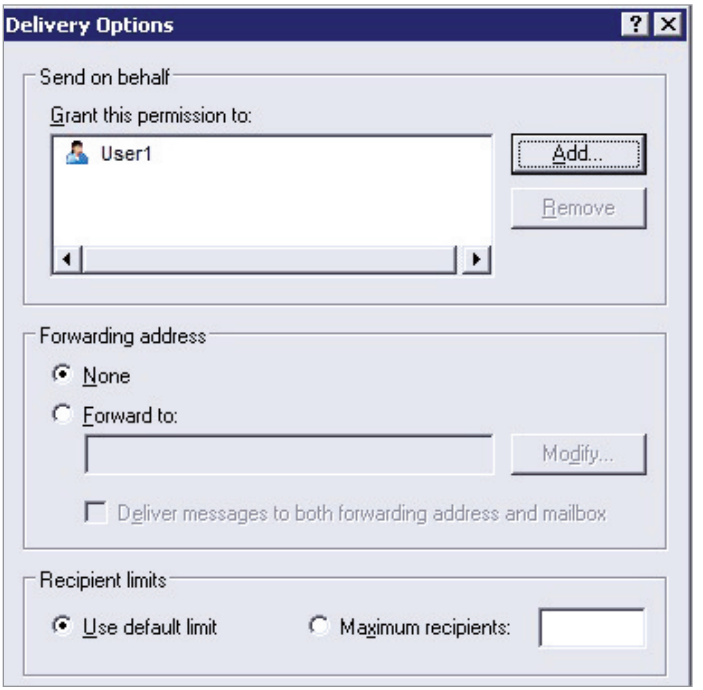
Another way to give Bob access to Sally's mailbox is to manually add Bob's AD username (user1) to Sally's *Send on behalf* permissions using either the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in or the Server Management console in Windows Server Essentials (formerly named Small Business Server). This method requires the involvement of an administrator, but not Bob or Sally.

Here are the steps that you or another administrator should follow to add Sally's AD username in the Active Directory Users and Computers snap-in:

1. On the Start menu, select Run, type dsa.msc, and click OK to access your domain's Active Directory Users and Computers snap-in.
2. Expand the appropriate domain and click the appropriate Users folder to open it. Double-click Sally's entry in the Users folder to open the Properties dialog box for Sally.
3. In Sally's Properties dialog box, select the Exchange General tab and click the Delivery Options button to open the Delivery Options dialog box. In the *Send on behalf* section, click the Add button. This will spawn the familiar AD selection dialog box in which you can select or enter an AD user or group. In this case,

select Bob's AD username and click OK. You'll now see Bob's AD username in the *Grant this permission to* box, as shown in Figure 5. Click the OK button to close the Delivery Options dialog box.

Figure 5
Granting Permission to Send Email on a User's Behalf



4. In Sally's Properties dialog box, select the Exchange Advanced tab. Click the Mailbox Rights button to bring up the Permissions dialog box, which contains the Mailbox Rights tab.

 Warning: If the Mailbox Rights tab contains only the SELF entry in the *Group or user names* box, don't add or edit any AD user. Instead, immediately click the Cancel button and see the Microsoft article "Mailbox Rights for New Users Shows Only Self" for corrective action before continuing to the next step.

5. Assuming that the *Group or user names* box doesn't contain only SELF, click the Add button to bring up the AD selection dialog box. Select or enter Bob's AD username and click OK. Bob's AD username (i.e., user1) will now appear in the *Group or user names* box, as shown in Figure 6.
6. Highlight Bob's AD username in the *Group or user names* box. In the *Permissions for User1* section, select the *Full mailbox access* check box. Click the OK button to close the Permissions dialog box.

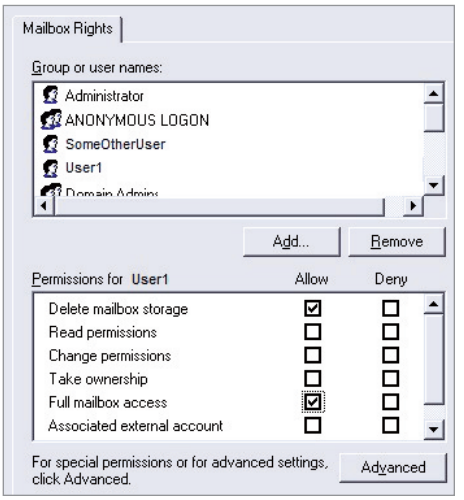


Figure 6
Granting Full Mailbox Access

After these steps are performed, Bob can access Sally's mailbox through the Other User's Folder option in his Outlook client. Like with Method 1, the email replies made by Bob to Sally's emails will include "on behalf of" in the From field.

Method 2 has the same disadvantage as Method 1. Bob can access only six folders (i.e., Calendar, Contacts, Inbox, Journal, Notes, and Tasks) and only one folder at a time.

Method 3

A third way to give Bob access to Sally's mailbox is to add Sally's Exchange profile to Bob's Windows Mail Profile. This method requires the involvement of an administrator, but not Bob or Sally (as long as the administrator has access to Sally's desktop). Here are the steps that you or another administrator should perform:

1. Grant Bob the *Send on behalf* and *Full mailbox* access permissions for Sally's mailbox using the Active Directory Users

There's no need to share Windows logon passwords just so someone can handle another person's Exchange mailbox.

and Computers snap-in, following steps 1 through 6 in the "Method 2" section.

2. Make sure that Bob is an Exchange user.

 Warning: If Bob isn't an Exchange user and an Exchange Profile is added to his Windows Mail Profile, Bob will lose various Outlook settings, including Rules and Alerts. In addition, the Outlook Calendar will be moved to the Exchange Calendar.

3. On Bob's PC, open the Control Panel and click the Mail icon. (If this icon isn't visible, change the *View by* option to either *Large icons* or *Small icons*.) Alternatively, you can access the Control Panel Mail applet by running the command

   ```
   control mlcfg32.cpl
   ```

 from Cmd.exe.
4. In the Mail Setup dialog box, click the Show Profiles button in the Profiles section. This will open the Mail dialog box, which contains only the General tab. A box labeled *The following profiles are set up on this computer* will already contain a highlighted profile called Default, Exchange, or some other name that was created by the person who originally configured Outlook as an Exchange client. Click the Properties button for the appropriate profile to open the Mail Setup dialog box for that profile.
5. In the Mail Setup dialog box, click the E-mail Accounts button to open the Account Settings dialog box. On the E-mail tab, highlight Microsoft Exchange Server and click the Change option in the tab's header. (Don't click the Change Folder button at the bottom.)
6. In the Change Account dialog box, click the More Settings button and select the Advanced tab. In the Mailboxes section, click the Add button.

7. In the Add User dialog box that appears, add Sally's Exchange profile using her short Windows user logon name and click OK. (Note that there's no lookup functionality available like you'd find in the Active Directory Users and Computers snap-in.) The Mailboxes section will then show her AD display name, as Figure 7 shows. Don't click the OK button just yet.

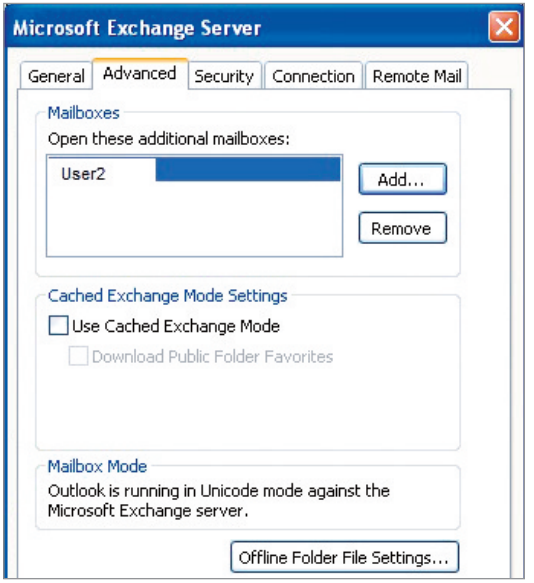


Figure 7
Adding an Exchange Profile

8. In the Cached Exchange Mode Settings section, leave the Use Cached Exchange Mode check box clear. If this option is enabled, Sally's mailbox will be cached locally on Bob's PC. This will not only generate a lot of network traffic but also take up disk space on Bob's PC and increase backup time.
9. Click OK to exit the Advanced tab of the More Settings dialog box.
10. In the Change Account dialog box, click the Next button at the bottom to continue. In the Congratulations dialog box, click the Finish button.
11. Click the Close button in the Account Settings and Mail Setup dialog boxes. In the Mail dialog box, click the OK button.

Now when Bob opens his Outlook client, he'll see his mailbox and Sally's mailbox, as Figure 8 shows. As in Method 1 and Method 2, the email replies made by Bob to Sally's emails will include "on behalf of" in the From field. When Bob replies to Sally's emails, the replies

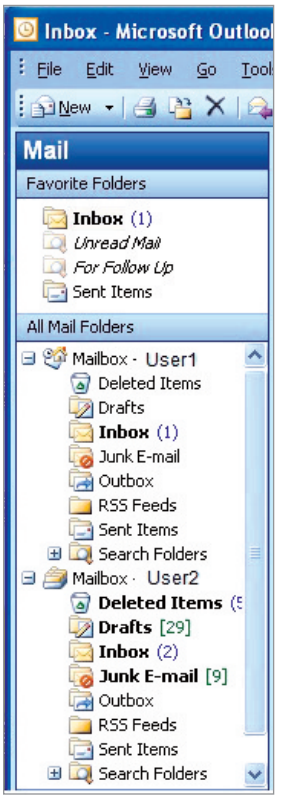


Figure 8
Seeing Both Users' Mailboxes in Outlook

are stored in Sally's Sent Items. Although users might not expect this, it's logical to store them there.

Method 3 offers two important advantages. First, Bob has full access to all of Sally's Outlook folders (not just the Calendar, Contacts, Inbox, Journal, Notes, and Tasks folders). Second, Bob can use the full functionality of the Outlook client to manage Sally's mailbox.

Methods to Avoid

There are two more ways to give Bob access to Sally's mailbox, both of which I don't recommend:

- *Using Microsoft Outlook Web Access (OWA).* With this method, Sally would give Bob her Windows logon credentials and Bob would use those credentials to open her mailbox in OWA. Although this approach takes the least amount of effort to accomplish, it's at the complete expense of network security. In addition, only one mailbox can be open at a time, no matter which web browser is being used. Evidently, OWA allows only one mailbox connection per PC ID or IP address. Finally, OWA isn't as feature rich as the Outlook client.
- *Using the Sharing option.* With this method, Sally would right-click her mailbox and select the Sharing option in Outlook 2003. However, this brings up a dialog box whose options are very confusing to configure. (In Outlook 2010, the same dialog box is reached by right-clicking the mailbox, clicking Folder permissions, and selecting the Permissions tab.) Plus, Outlook doesn't offer any help on configuring the options in this dialog box, not even when F1 is pressed.

Three Methods Lead to Same Successful Result

Having a manager, co-worker, or assistant manage an absent employee's Exchange email account is commonplace and necessary. Email access can quickly be provided, without compromising the absent employee's entire desktop. There's absolutely no need to share Windows logon passwords just so someone can handle another person's Exchange mailbox. Employees will also appreciate that they don't have to bounce from desk to desk many times a day to respond to absent employees' email messages.

In addition, the "on behalf of" insertion in the From field ensures that the manager, co-worker, or assistant can't use the absent employee's email without his or her knowledge, preventing intentional nefarious behavior. The "on behalf of" insertion also prevents confusion in the future as to who actually created the email content.

As you've seen, there are three recommended methods for allowing a user to access another user's Exchange mailbox. Method 1 allows users to delegate authority, albeit with limited access to the absent employee's entire Exchange folder structure. Method 2 provides the same capabilities as Method 1 and might be more appropriate for non–technical-savvy users. For users, Method 3 is just like sitting in the absent employee's chair. Plus, it's the best method for administrators who need complete control. No matter which recommended method you choose, it takes less than three minutes to implement it once you know what you're doing. ■

FAQ

Answers to Your Questions



John Savill



Jan De Clercq

Q: What is the new Distributed Key Management (DKM) feature in Microsoft System Center Virtual Machine Manager (VMM) 2012?

A: The VMM database contains sensitive information, such as product keys and administrator passwords. To protect the contents of this database, VMM uses encryption. By default, the cryptographic keys needed to access the encrypted data are stored locally on the VMM server. However, in a clustered VMM server setup, both cluster nodes might need to access the same encryption keys, so the keys can't be stored on a single cluster node. That's why Microsoft introduced the DKM feature in VMM 2012. Instead of storing the keys locally on the server, DKM lets you store them in a special container named VMMDKM in Active Directory (AD).

You can configure DKM when you're installing a VMM management server with the Virtual Machine Manager Setup Wizard. On the *Configure service account and distributed key management* page of the wizard, you simply need to select the *Store my keys in Active Directory* check box and provide the location of the DKM container in AD. For example, for a domain named windowsitpro.net, you'd specify CN = VMMDKM,DC = windowsitpro,DC = net. If the account you're using to install VMM has permission to create new containers in AD, the VMM installation automatically creates the VMMDKM container. If that's not the case, you can manually create the container in AD before starting the VMM installation. (You can use ADSI Edit to create it.) Also make sure that the account with which you're installing VMM has full control permission to the VMMDKM container. For

more information about DKM and how to set it up, see the Microsoft TechNet article "Configuring Distributed Key Management in VMM."

—Jan De Clercq

Q: Can I pre-provision BitLocker Drive Encryption for a Windows 8 volume from a standard Windows Preinstallation Environment (WinPE) image by using the command-line utility Manage-bde?

A: No, it's not possible to use Manage-bde from a standard Windows Preinstallation Environment (WinPE) image because, by default, WinPE doesn't include Manage-bde and the Windows Management Instrumentation (WMI) objects it leverages. To create the custom WinPE image for a Windows 8 volume, you must add the WinPE-WMI and WinPE-SecureStartup optional components in the WinPE image. The following Microsoft articles describe how to add these components:

- "Building a Windows PE Image with Optional Components"
- "How to Add an Optional Component to Windows PE"

If you're unfamiliar with pre-provisioning BDE, see "New BitLocker Features Speed Up the Encryption Process in Windows 8."

—Jan De Clercq

Q: Why am I getting an error when using Windows PowerShell to make a Windows Server 2012 Hyper-V host be Live Migration–enabled?

A: If a host is enabled for Live Migration, then its Virtual MachineMigrationEnabled attribute is set to true:

```
PS C:\> (Get-VMHost savdalhv01).VirtualMachineMigrationEnabled
True
```

However, if you try to enable Live Migration by setting this value, you will get an error message saying that this attribute is read-only. To enable Live Migration, you need to use the Enable-VMMigration cmdlet:

```
PS C:\> Enable-VMMigration
```

Additionally , you might want to set the networks that can be used for Live Migration by using the Set-VMMigrationNetwork cmdlet:

```
PS C:\> Set-VMMigrationNetwork 10.1.2.1
```

You also might consider setting the authentication method by using the Set-VMHost –VirtualMachineMigrationAuthenticationType. My example sets it for Kerberos:

```
PS C:\> Set-VMHost –VirtualMachineMigration
  AuthenticationType Kerberos
```

—John Savill

Q: What are the Windows Azure Infrastructure as a Service rights as part of my MSDN subscription?

A: With MSDN subscriptions, you receive numerous benefits, including Windows Azure services. The actual prices vary depending on whether the MSDN subscription is Professional, Premium, or Ultimate. Full details can be found at the MSDN benefits site.

To give an idea of what Infrastructure as a Service (IaaS) rights this equates to, let's look at the Ultimate subscription, which offers 1,500 Small Standard instance hours. Considering an average month of 30 days has 720 hours, a small virtual machine (VM) (which has a single dedicated core) that exists all month would use 720 Small Standard hours.

This means the MSDN Ultimate subscription would let you run two small VMs all month. The MSDN Premium subscription, which gives 750 hours, would let you run one small VM all month.

Remember, VMs consume hours, whether the VM is running or not. During the time the VM exists, it consumes resources, so if you want to save your hours, make sure you delete unused VMs.

—John Savill

Q: How can I control the placement of Start Screen tiles in Windows 8?

A: In Windows 8, there's no way to control the tiles placed on the Start Screen by using Group Policy or other means. It's not a capability native to the OS. The best approach is to give users some basic training on how to customize options, so they can tweak the Start Screen to their exact needs. The goal of the Start Screen is for users to customize it to their needs, which is why I believe there's no IT control possible after deployment.

However, it's possible to customize the Start Screen as part of your base image that gets deployed to your environment. Additionally, in the unattend answer file (unattend.xml) there's a section, Microsoft-Windows-Shell-Setup\StartTiles, that has some customization of the Start Screen (documented at TechNet) but there's no post-deployment IT customization.

—John Savill

Q: What is the purpose of the new DHCP guard feature in Windows Server 2012 Hyper-V?

A: DHCP guard is a new property in Windows Server 2012 Hyper-V that you can configure for each network adapter in a virtual machine (VM). When DHCP guard is enabled, it prevents a VM from acting as a DHCP server. If a VM attempts to send

a packet that indicates it's a DHCP server, the packet will automatically be dropped.

You can enable DHCP guard using Server 2012 Hyper-V Manager. In the VM's properties, go to the Network Adapter settings and click

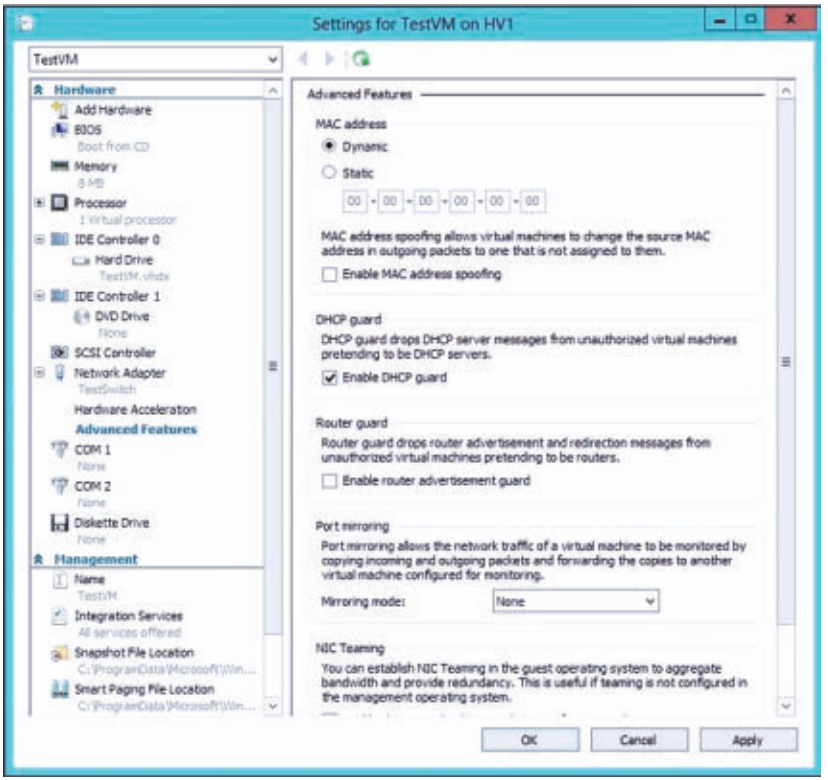


Figure 1
Enabling DHCP Guard in Server 2012 Hyper-V Manager

Advanced Features. Select the Enable DHCP guard check box, as Figure 1 shows. I recommend that you enable this setting during the creation of your VM golden image. That way, it's enabled by default for all new VMs you create from that image. ■

—Jan De Clercq

Best of TechEd 2013 Award Winners



Jason Bovberg

Email

Twitter

Website

At Microsoft TechEd 2013 in New Orleans, our editors honored this year's Best of TechEd Award winners. This 10-year-old program has become a highly regarded—and sometimes very competitive!—program, but over the years it has recognized some excellent products. As always, our main criteria for these awards are the products' strategic importance to the market, competitive advantage, and value to the customer.

This year, our judging panel narrowed an impressive field of more than 250 submissions down to 32 finalists in 10 judged categories and 3 additional categories—Breakthrough Technology, Attendees' Pick: Microsoft, and Attendees' Pick: Microsoft Partner. And this year, we had the opportunity to call out Microsoft products in a few categories, where we believe Microsoft itself deserved special recognition. Congratulations to our 2013 Best of TechEd winners!



Veeam Software's Doug Hazelman

Backup and Recovery

Veeam Backup & Replication 6.5

Veeam Backup & Replication provides essential backup and replication for an increasingly virtualized world. Instead of merely tolerating the virtual environment, Veeam leverages it to provide the most comprehensive protection for the virtual infrastructure.

Cloud Computing

Optimal IdM's Virtual Identity Server for Office 365

Optimal IdM's Virtual Identity Server (VIS) for Office 365 solves a rapidly growing need among IT environments—seamlessly connecting companies to Office 365—and doing it elegantly. By lowering the friction of using Office 365, it allows companies to rapidly take advantage of this popular service.

Special Microsoft recognition in this category: Windows Azure

Database

Idera's SQL toolbox

Idera's SQL toolbox is a powerful collection of database management tools that perform monitoring, diagnostics, and troubleshooting. This product won simply because it addresses the entire range of day-to-day issues faced by DBAs and database professionals.

Special Microsoft recognition in this category: SQL Server 2012

Hardware

A10 Networks' A10 Thunder Series

A10 Networks' A10 Thunder appliances are exquisitely designed hardware and software Application Delivery Controllers (ADCs). This series won the category thanks to the bevy of innovations inside the hardware and software that make cloud applications faster, more flexible, and more secure, with intelligent services convergence. The A10 Thunder platform's compact size, streamlined performance, and green efficiency are unprecedented.

Messaging and Unified Communications

StorageCraft ShadowProtect Granular Recovery for Exchange

Email is the most business-critical function. Having the ability to restore single email messages or complete mailboxes in real time means the business runs uninterrupted. StorageCraft fills a significant void in total messaging management.

Security

Proofpoint Targeted Attack Protection

Proofpoint Targeted Attack Protection addresses a desperate need most companies have: protection against targeted email malware attacks known as spearphishing. Using very sophisticated detection and mitigation techniques, this product significantly reduces a company's vulnerability from the main attack vector in company penetrations.

SharePoint

AvePoint's DocAve 6

AvePoint's DocAve 6 is a full-service solution for SharePoint, providing migration services with full reporting and security mirroring. DocAve stood out as a complete solution for migrating and managing SharePoint implementations not only between servers but also from on-premises to the cloud. The level of granularity and customization for migrations is a value for any company managing large SharePoint farms.

Software Development

Telerik's DevCraft

Telerik's DevCraft is a full-featured suite of tools and controls for Windows, web, and mobile development. It won this category because it offers the broadest range of tools, covering the entire software development lifecycle.

Systems Management

NetApp's FlexPod with Microsoft Private Cloud

A collaborative effort between NetApp, Cisco, and Microsoft, NetApp's FlexPod combines hardware and software to provide a complete turnkey solution for Hyper-V provisioning. The FlexPod software toolkit utilizes PowerShell and Orchestrator to minimize customer headaches by fully automating the provisioning process. This product provides a strong level of support and future potential.

Virtualization

Cisco Nexus 1000V Switch for Microsoft Hyper-V

The Cisco Nexus 1000V Switch for Microsoft Hyper-V is a virtual network switch specifically for Microsoft's Hyper-V. The product won this category because it brings enterprise-class networking to the Hyper-V virtualization platform and extends Hyper-V networking across the private and public cloud.

Special Microsoft recognition in this category: Hyper-V Server

Breakthrough Product

Lenovo's ThinkPad Helix Ultrabook Convertible

The Lenovo ThinkPad Helix is one of the very best in the first wave of innovative Windows 8 hybrid devices, demonstrating the power, creativity, and functionality that's possible in the new age of performance-focused touch computing.



Intel's Eduardo Campoy receiving the award for the Lenovo ThinkPad

Attendees' Pick: Microsoft

Microsoft Hyper-V Server 2012

In our newest category, in which attendees chose their favorite Microsoft product from a selection of nominated products, Microsoft Hyper-V Server 2012 took top prize. Microsoft's hypervisor-based server virtualization product continues to rise in stature, consolidating workloads, helping organizations improve server utilization, and reducing costs.

Attendees' Pick: Microsoft Partner

A10 Networks' A10 Thunder Series

Attendees agreed with our selection of the A10 Thunder appliances in the Hardware category, bestowing the popular pick to these finely designed, comprehensively featured hardware and software solutions. ■

Product News for IT Pros

NEC Integrates with System Center 2012 and Windows Server 2012

The NEC ProgrammableFlow Network Suite is optimized to integrate with Microsoft System Center 2012 Virtual Machine Manager (VMM), delivering automated server and network orchestration for virtualized data centers. This new integrated solution promises to transform network management for Windows Server 2012 customers, enabling new levels of control, flexibility, and automation. NEC's planned SDN solution will help customers of Server 2012 and Hyper-V automate the time-consuming and disruptive task of configuring their networks as they support the dynamic movement of virtual machines (VMs). The product further enhances the flexibility provided by the complete network virtualization introduced with the NEC OpenFlow-based vSwitch for Windows Server 2012 Hyper-V. NEC's ProgrammableFlow vSwitch for Windows Server Hyper-V environments, the PF1000, and the ProgrammableFlow SDN Controller manage network flows, working in conjunction with VMM and controlling the source and destination VMs. For more information, check out the NEC website.

SolarWinds NPM Offers Network Route and Multicast Monitoring

SolarWinds introduced new network route and multicast monitoring capabilities within its flagship network management product, SolarWinds Network Performance Monitor (NPM). SolarWinds NPM offers IT pros powerful network fault, availability, and performance management, simplifying detection, diagnosis, and resolution of network issues before outages occur. As today's dynamic networks grow in size and complexity, the number of active routing topology states grows

exponentially. With its new network route monitoring feature, SolarWinds NPM takes fault and performance monitoring to a new level by providing real-time network route information alongside device status and performance statistics. With the product's support for major routing protocols, IT pros can now view routing tables, changes in default routes, Border Gateway Protocol (BGP) transitions, and flapping routes in an intuitive web-based console. For more information, including a free downloadable 30-day trial, visit the SolarWinds website.

SXR Software

SXR Software Gets User Activity Under Control

SXR Software announced the release of StatWin Server Enterprise 9.0, a new version of its employee monitoring and time tracking software. This program remotely monitors and records keystrokes, mouse actions, and running applications; it also measures the efficiency of each user and time spent on each task. StatWin Server Enterprise aims to solve many potential problems of employee monitoring and workflow control, even before they appear. By monitoring user activity and network traffic, the program effectively tracks all significant events taking place in the corporate network and on individual machines. The new StatWin Server Enterprise 9.0 introduces a range of additional user activity control features, including an Intensity parameter varying from 1 to 10, indicating how intensively a user worked in the given period, as well as an automatic IP scanner to quickly retrieve computer names in the network. For more information, visit the SXR Software website.

serverLIFT®

ServerLIFT SL-1000X Gives Your Equipment a Lift

The SL-1000X Powered ServerLIFT is the best-in-class solution for handling the most challenging and heaviest IT equipment in today's data center environment. Positioned as the only compact lift that is rated for 1,000 pounds, the SL-1000X super duty server lift is designed to meet the growing demands of the constantly evolving IT industry. The SL-1000X easily navigates the narrowest data center aisles, with a slim footprint. Its side-loading operability allows for convenient

equipment loading from either side of the lift. The unit features a heavy-duty platform that maintains stability to ensure precise alignment under maximum loads. The ServerLIFT-exclusive extending shelf enables seamless installation, preventing injury and dropped equipment. The SL-1000X empowers your data center and prepares your enterprise for scalability to meet current and future IT trends. For more information, check out the ServerLIFT website.

Druva Could Save You Hours of Migration Time

Druva introduced a settings-backup capability in its inSync endpoint data protection platform that will save hundreds of hours of IT overhead for enterprises confronting the task of upgrading corporate PCs when Windows XP is sunsetted in April 2014. The new Persona Backup feature enables system and application settings to be saved and restored with a click by end users themselves. Combining the new feature with inSync's core endpoint data backup/restore abilities not only slashes migration downtime but also allows end users to perform their own device migrations without IT intervention. With XP still expected to power over 30 percent of all Windows PCs when Microsoft issues its final security update for the 12-year-old OS next year, inSync will provide an easy migration path to Windows 7/Windows 8 that eliminates manual transfer of data and settings. The inSync platform can also streamline any other OS, device, or hardware platform migration scenario, including moving data and settings from laptop to laptop, laptop to tablet, and Windows to Mac, as well as simplify the process of rebuilding damaged hardware and replacing lost or stolen devices. For more information about inSync's ability to simplify OS and other migration, visit the Druva website.

Kroll Ontrack Embraces eCommerce for Ontrack Eraser 4.0

Kroll Ontrack announced a new subscription-based pricing model for its enterprise data eraser solution, Ontrack Eraser 4.0. Starting at $99.95, the new model offers customers a simple and flexible way to

meet the specific data erasing needs of their business by purchasing the solution directly from the Kroll Ontrack online shop. Full software functionality includes VMware Drive Wiping Capabilities (the ability to delete data from VMware machines, ensuring that corporations are securely deleting data from their virtual environments and therefore addressing the complete scope of their IT environment), enhanced system performance (the ability to perform more than 200 concurrent device erasures), enhanced system reporting (new reports that denote the hard drive make, serial number, and model number, as well as the wipe algorithm applied to accomplish the job), and security and central management capabilities (new system authentication functionality to ensure that the erasure is conducted in the correct manner by the appropriate individual). For more information about Ontrack Eraser 4.0, the Kroll Ontrack website.

Skybot Software Job Scheduler Integrates Oracle E-Business Suite Requests

Skybot Software announced the release of Skybot Scheduler 3.3, which includes an Oracle E-Business Suite (EBS) interface that allows users to easily build complex schedules for EBS concurrent requests within Skybot Scheduler. Oracle EBS requests also can be included in centralized job scheduling across multiple systems and applications, such as backups or file transfers, without additional scripting. "The original challenge of server sprawl has been compounded by an equally growing diversity of applications," said Janet Dryer, CEO of Help/Systems (parent company of Skybot Software). "With IT departments at their leanest, job schedulers that can bridge the gap between systems and applications are critical." Since introducing Skybot Scheduler in September 2010, Skybot Software has released 17 version enhancements, including three major product updates. For more information, visit the Skybot Software website. ■

Directory of Services

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
forums.windowsitpro.com

News

Check out the current news and information about Microsoft Windows technologies.
www.winsupersite.com

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- Cloud & Virtualization UPDATE
- *Dev Pro* UPDATE
- Exchange & Outlook UPDATE
- Security UPDATE
- *SharePoint Pro* UPDATE
- *SQL Server Pro* UPDATE
- *Windows IT Pro* UPDATE
- WinInfo Daily UPDATE

RELATED PRODUCTS

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events plus a subscription to either *Windows IT Pro* or *SQL Server Pro*.
windowsitpro.com/vip-premium-membership

SQL Server Pro

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

Dev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

Advertiser Directory

1&1 Internet 1

AvePoint 2

IT/Dev Connections 6

Vendor Directory

A10 Networks 66, 68

Amazon 26

Apple 22

AvePoint 67

Cisco 14, 67, 68

Citrix 22

Druva 71

Google 22

Idera 66

Kroll Ontrack 71, 72

Lenovo 68

NEC 69

NetApp 67

Optimal IdM 66

Proofpoint 67

ServerLIFT 70, 71

Skybot Software 72

SolarWinds 69, 70

Stardock 18

StorageCraft Technology 66

SXR Software 70

Telerik 67

Veeam Software 65

VMware 14, 22, 39, 40, 41, 42, 45, 46, 47, 49, 50

Windows IT Pro